

I, SHAUN WU, hereby declare:

That I possess advanced knowledge of the Japanese and English languages. The attached Japanese into English translation has been translated by me and to the best of my knowledge and belief, it is a true and accurate translation of the Japanese Patent Publication No. 2004-166153.

I declare that all statements made above of my own knowledge are true and that all statements made on information and belief are believed to be true. I have been warned and understand that willful false statements and the like are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code.

I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct.

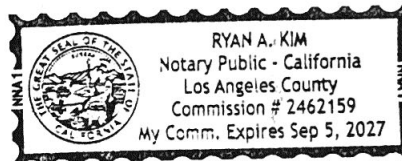
Executed on May 14, 2024 in Los Angeles, California.

Shaun Wu

Notary Public

Notary Commission Expiry

09/05/2027



(19) Japan Patent Office (JP)

(12) Japanese Unexamined Patent
Application Publication (A)(11) Patent Application
Publication Number
Laid-Open Patent Application
No. 2004-166153
(P2004-166153A)(43) Publication Date: **June 10, 2004 (2004.6.10)**

(51) Int.C1.7	F1			Theme Code (Reference)
HO4L 9/08	HO4L9/00	601B	5J1O4	
HO4L 9/14	HO4L9/00	641		

Request for Review: Yes**Number of Claims: 8 OL (Total 25 pages)**

(21) Application Number JP2002-332404 (P2002-332404)
 (22) Application Date November 15, 2002 (2002.11.15)

(71) Applicant 000004237
 NEC Corporation
 5-7-1 Shiba, Minato-Ku, Tokyo

(71) Applicant 000232254
 NEC Communication Systems, Ltd.
 1-4-28 Mita, Minato-Ku, Tokyo

(74) Agent 100088890
 Patent Attorney: Junichi Kawahara

(72) Inventor Kazuya Suzuki
 NEC Corporation, 5-7-1 Shiba, Minato-Ku, Tokyo

(72) Inventor Jibiki Masahiro
 NEC Corporation, 5-7-1 Shiba, Minato-Ku, Tokyo

Continue to the last page

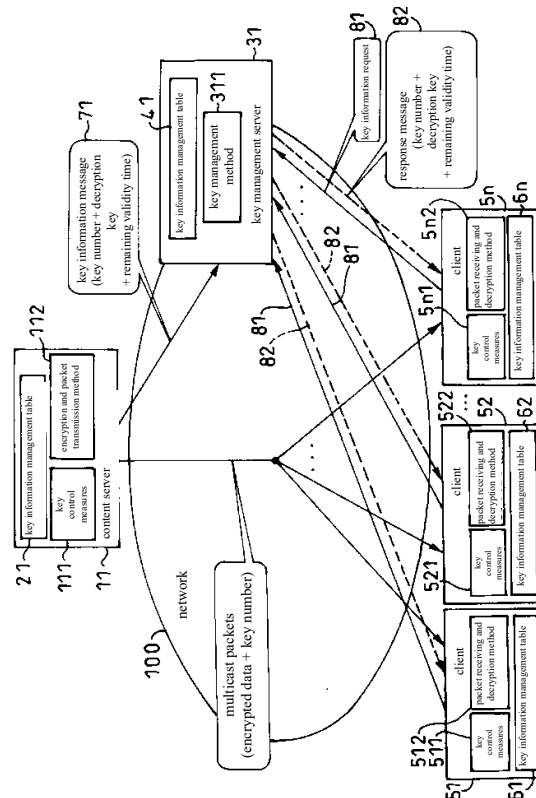
(54) [Name of Invention] KEY EXCHANGE METHOD IN MULTICAST DISTRIBUTION SYSTEM

(57)[Abstract]

[Problem] The present invention aims to avoid processing delays that occur when a client acquires a new decryption key during key change (exchange).

[Solution] A content server distributes a decryption key to be used next to a key management server within the validity time of the key currently in use, and transmits a multicast packet including the key number. Each of the clients 51 to 5n requests the key management server 31 to transmit the next decryption key to be used within the validity time of the key currently in use and after the content server 11 has distributed the next decryption key to be used to the key management server 31. Also, the encrypted data in the multicast packet is decrypted using a decryption key corresponding to the key number in the multicast packet. The key management server 31 receives the next decryption key to be used from the content server 11, and in response to a transmission request from each of the clients 51 to 5n, transmits the next decryption key to be used to the source of the request.

[Selected Drawing] Figure 1



CLAIMS

[Claim 1]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a content server that creates an encryption key/decryption key, manages the encryption key/decryption key and its key number and remaining validity time, distributes the decryption key to be used next to the key management server within the validity time of the key in use, and transmits a multicast packet containing encrypted data and the key number of the encryption key used in the encryption;

a client that requests the key management server to transmits the decryption key to be used next within the validity time of the key in use after the content server distributes the decryption key to be used next to the key management server, and decrypts the encrypted data in the multicast packet using the decryption key corresponding to the key number in the multicast packet received from the content server; and

10

the key management server that manages the the decryption key, its key number and remaining validity time, receives a decryption key to be used next from the content server, and transmits the decryption key to be used next to the client in response to a request from the client.

[Claim 2]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a content server that manages the encryption key, its key number, and remaining validity time, requests the key management server to create the next encryption key/decryption key within the validity time of the key in use, receives the encryption key created in response to the request from the key management server, transmits a multicast packet containing encrypted data and the key number of the encryption key used in the encryption;

20

a client that requests the key management server to transmit the decryption key to be used next after the content server requests the key management server to create an encryption key/decryption key to be used next within the validity time of the key in use, decrypts the encrypted data in the multicast packet using the decryption key corresponding to the key number in the multicast packet received from the content server; and

the key management server that manages the encryption key, decryption key, their key numbers and remaining validity time, creates and stores an encryption key/decryption key to be used next in response to a request from the content server, and transmits the encryption key to be used next to the content server, and transmits the decryption key to be used next to the client in response to a request from the client.

[Claim 3]

A key exchange method in a multicast distribution system according to claim 1 or 2, wherein the address of a key management server is added to the information in a multicast packet transmitted from a content server to a client, thereby eliminating the need for the client to set a destination for querying and requesting a decryption key.

30

[Claim 4]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a key information management table in the content server that stores a set of the encryption key/decryption key in use, its key number, and its remaining validity time, and a set of the encryption key/decryption key to be used next, its key number, and its remaining validity time;

a key management means within the content server that transmits a key information message regarding the decryption key to be used next to the key management server when the remaining validity time of the key in use reaches the first setting value, switches the key stored in the table as the next key to be used to the new key in use when the remaining validity time of the key in use reaches 0, creates a new encryption key/decryption key to be used next and saves the key information in the table;

an encryption/packet transmission means within the content server that encrypts the distributed data using the encryption key in use stored in its table at the time of multicast distribution, transmits a multicast packet containing encrypted data and the key number of the encryption key;

40

a key information management table in the client that stores a set of the decryption key in use, its key number, and its remaining validity time, and can store a set of the decryption key to be used next, its key number, and its remaining validity time;

a packet receiving/decryption means within the client that receives multicast packets sent from the content server, searches the decryption key from its table according to the key number in the received multicast packet, and decrypts the encrypted data in the multicast packet using the decryption key of that key number;

a key management means within the client that transmits a key information request to the key management server when the remaining validity time of the key in use reaches the second setting value, saves the set of the decryption key to be used next, its key number, and its remaining validity time in the response message in its own table, and switches the key that was previously stored in the table as the next key to be used to the new key in use based on the recognition of changes in key numbers in multicast packets sent from the content server;

10

a key information management table in the key management server that can store a set of the decryption key in use, its key number, and its remaining validity time, and can store a set of the decryption key to be used next, its key number, and its remaining validity time;

and a key management means within the key management server that saves a set of the decryption key to be used next, its key number, and its remaining validity time in the key information message received from the content server in its table, transmits a response message containing a set of the decryption key to be used next, its key number, and its remaining validity time back to the client when receiving a key information request from the client when the remaining validity time of the key in use reaches the second setting value, switches the key stored in the table to the new key as the next key to be used when the remaining validity time of the key in use reaches 0.

[Claim 5]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

20

a key information management table in the content server that can hold a set of the encryption key in use, its key number, and its remaining validity time, and can also hold a set of the encryption key to be used next, its key number, and its remaining validity time;

a key management means within the content server that issues a key creation request requesting the key management server to create the next key to be used when the remaining validity time of the key in use reaches the first setting value, saves the set of the encryption key to be used next, its key number, and its remaining validity time in the key information response message in its own table, and switches the key stored in the table to the new key as the next key to be used when the remaining validity time of the key in use reaches 0;

an encryption/packet transmission means within the content server that encrypts the distributed data using the encryption key in use stored in its own table at the time of multicast distribution, transmits a multicast packet containing encrypted data and the key number of the encryption key;

a key information management table in the client that stores a set of the decryption key in use, its key number, and its remaining validity time, and can store a set of the decryption key to be used next, its key number, and its remaining validity time;

30

a packet receiving/decryption means within the client that receives multicast packets sent from the content server, searches the decryption key from its table according to the key number in the received multicast packet, and decrypts the encrypted data in the multicast packet using the decryption key of that key number;

a key management means within the client that transmits a key information request to the key management server when the remaining validity time of the key in use reaches the second setting value, saves the set of decryption key to be used next, its key number, and its remaining validity time in the response message in its table, and switches the key that was previously stored in the table as the next key to be used to the new key in use based on recognition of changes in key numbers in multicast packets sent from the content server;

a key information management table in the key management server that can store a set of the encryption key/decryption key in use, its key number, and its remaining validity time, and can also store a set of the encryption key/decryption key to be used next, its key number, and its remaining validity time; and

40

50

a key management means within the key management server that creates the encryption key/decryption key to be used next in response to the key creation request from the content server, saves the set of the encryption key/decryption key to be used next, its key number, and its remaining validity time in its table, returns a key information response message regarding the encryption key to be used next to the content server, transmits a response message containing a set of the decryption key to be used next, its key number, and its remaining validity time back to the client, and switches the key stored in the table to the new key as the next key to be used when the remaining validity time of the key in use reaches 0.

[Claim 6]

A key exchange method in a multicast distribution system according to claim 4 or claim 5, wherein the address of a key management server is added to the information in a multicast packet transmitted from a content server to a client, thereby eliminating the need for the client to set a destination for a key information request.

10

[Claim 7]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a content server key exchange control program in which the content server functions as

a key information management table that stores a set of an encryption key/decryption key in use, its key number, and its remaining validity time, and a set of an encryption key/decryption key to be used next, its key number, and its remaining validity time,

a key management means in which when the remaining validity time of the key in use reaches the first setting value, it transmits a key information message regarding the decryption key to be used next to the key management server and when the remaining validity time of the key in use reaches 0, switches the key stored in its own table as the next key to be used to a new key in use, creates a new encryption key/decryption key to be used next, and saves the key information in its own table, and

20

an encryption/packet transmission means that encrypts distributed data using the currently used encryption key stored in its own table during multicast distribution, and transmits a multicast packet containing the encrypted data and the key number of the encryption key;

a client key exchange control program in which the client functions as

a key information management table capable of holding a set of a decryption key in use, its key number, and its remaining validity time, and a set of a decryption key to be used next, its key number, and its remaining validity time,

a packet receiving/decryption means that receives a multicast packet sent from a content server, searches for a decryption key from its own table using the key number in the received multicast packet, and decrypts the encrypted data in the multicast packet using the decryption key with that key number, and

a key management means in which when the remaining validity time of the key in use reaches the second setting value, it transmits a key information request to the key management server, saves the set of the decryption key to be used next, its key number, and its remaining validity time in the response message in its own table, and switches the key that was previously stored in its own table as the next key to be used to the new key in use based on the recognition of changes in key numbers in multicast packets sent from the content server; and

30

a key exchange control program for the key management server in which the key management server functions as

a key information management table capable of storing a set of a decryption key in use, its key number, and its remaining validity time, and a set of a decryption key to be used next, its key number, and its remaining validity time, and

a key management method that saves a set of the decryption key to be used next, its key number, and its remaining validity time in the key information message received from the content server in its own table, transmits a response message containing a set of the decryption key to be used next, its key number, and its remaining validity time back to the client in response to the key information request from the client when the remaining validity time of the key in use reaches the second setting value, and switches the next key to be used from the key stored in the own table to the new key in use when the remaining validity time of the currently used key reaches 0.

40

[Claim 8]

A key exchange method in multicast distribution system having a network system where multicast distribution of encrypted data is performed, comprising:

a content server key exchange control program in which the content server functions as

50

a key information management table capable of storing a set of an encryption key in use, its key number, and its remaining validity time, and a set of an encryption key to be used next, its key number, and its remaining validity time,

a key management means that issues a key creation request to the key management server to request creation of the next key to be used when the remaining validity time of the key in use reaches a first setting value, saves the set of the encryption key to be used next, its key number, and its remaining validity time in the key information response message received as a response in its own table, and switches a key stored in its own table to a new key to be used next when the remaining validity time of the key in use reaches 0, and

an encryption/packet transmission means that encrypts distribution data using an encryption key in use stored in its own table during multicast distribution, and transmits a multicast packet having the encrypted data and the key number of the encryption key;

10

a client key exchange control program in which the client functions as

a key information management table capable of storing a set of a decryption key in use, its key number, and its remaining validity time, and a set of a decryption key to be used next, its key number, and its remaining validity time,

a packet receiving/decryption means that receives a multicast packet sent from a content server, searches for a decryption key from its own table using the key number in the received multicast packet, and decrypts the encrypted data in the multicast packet using the decryption key with that key number,

a key management means that transmits a key information request to the key management server when the remaining validity time of the key in use reaches the second setting value, saves the set of the decryption key to be used next, its key number, and its remaining validity time in the response message in its own table, and switches the key that was previously stored in the local table as the next key to be used to the new key in use based on the recognition of changes in key numbers in multicast packets sent from the content server; and

20

a key exchange control program for the key management server in which the key management server functions as

a key information management table that can store a set of the encryption key/decryption key in use, its key number, and its remaining validity time and can also store a set of the encryption key/decryption key to be used next, its key number, and its remaining validity time, creates the encryption key/decryption key to be used next in response to the key creation request received from the content server, saves the set of the encryption key/decryption key to be used next, its key number, and its remaining validity time in its own table, transmits back a key information response message regarding the encryption key to be used next to the content server, transmits back a response message containing a pair of the decryption key to be used next, its key number, and its remaining validity time to the client when a key information request is received from the client when the remaining validity time of the key in use reaches the second setting value, and switches the key stored in its own table to a new key to be used next when the remaining validity time of the currently used key reaches 0.

DETAILED DESCRIPTION OF THE INVENTION

30

[0001]

[Technical Field]

The present invention relates to a multicast distribution system that prevents eavesdropping by encrypting multicast distribution using a different key at regular intervals, and to a key exchange method in a multicast distribution system for controlling and managing the exchange of keys (encryption key/decryption key).

[0002]

[Conventional Technology]

Generally, multicast packets are received by an unspecified number of recipients, so in order to allow only specific clients to view them, the data delivered by the packets must be encrypted with an encryption key and a decryption key must be distributed only to clients permitted to view them.

[0003]

At this time, by periodically changing the key, it is possible to manage clients and further improve the confidentiality of the encryption.

40

[0004]

Conventionally, in multicast distribution systems in which distribution data (data to be distributed) is encrypted, encryption keys and decryption keys have been replaced to prevent eavesdropping by encrypting the data using different keys at regular intervals (see, for

50

example, Patent Document 1).

[0005]

Such a conventional multicast distribution system includes a content server (referred to as a "transmitter" in Patent Document 1), a client (referred to as a "receiver" in Patent Document 1), and a key management server. The content server transmits a packet with key request information attached at regular intervals. The client that receives this information requests a key from the key management server, which updates the key at regular intervals, preventing the encrypted data from being leaked even if the key falls into the hands of a third party.

[0006]

[Patent Document 1]

JP2001-285273A (pages 2-4, FIG. 1)

10

[0007]

[Problem To Be Solved by The Invention]

The above-mentioned key exchange method in the conventional multicast distribution system has the following problems.

[0008]

The first problem is that a time lag occurs when receiving key request information. The reason for this problem is that when a client receives key request information, it requests a key from the key management server and starts decryption only after receiving the response (key). and the client cannot decrypt the encrypted information (encrypted data) until a response is received from the key management server.

[0009]

The second problem is that if a user joins a multicast broadcast in the middle of a broadcast, the user cannot view the broadcast immediately. The reason for this problem is that packets with attached key request information are generated at regular intervals, so clients participating in a multicast broadcast cannot obtain the decryption key until the next key request information is sent, and therefore cannot decrypt the data.

20

[0010]

The third problem is that when the key request information distributed by multicast is lost on the route, the key cannot be obtained for a long period of time. The reason for this problem is that multicast delivery does not perform confirmation, so it is not possible to check if a packet has been lost along the route. Therefore, if a packet with a key request attached is lost, a new key cannot be obtained until the next key request is sent. Thus, the encrypted information cannot be decrypted until the new key is available.

[0011]

In view of the above, the object of the present invention is to solve the above problems and to provide a key exchange method in a multicast distribution system that prevents eavesdropping by encrypting data with a different key at regular intervals during multicast distribution, thereby eliminating the confirmation delay (key switch delay) that occurs when changing (exchanging) a key and enabling real-time data processing.

30

[0012]

In other words, the feature of the present invention is that when encryption of distribution data during multicast distribution is performed, the encryption key and decryption key are changed periodically to improve the confidentiality of the encryption, and it is also possible to prevent delays associated with the acquisition (by the client) of new key information (the key and associated information) when the key is changed.

[0013]

[Means For Solving the Problem]

The key exchange method in the multicast distribution system related to the present invention has a network system where multicast distribution of encrypted data is performed, comprising:

a key information management table in the content server that stores a set of the encryption key/decryption key in use (paired encryption key and decryption key; they may be the same key), its key number (information for identifying the key), and its remaining validity time (key information related to the key), the encryption key/decryption key to be used next, its key number, and its remaining validity time;

40

a key management means in the content server that transmits a key information message regarding the decryption key to be used next to the key management server (a message containing key information that is a set of the decryption key to be used next, its key number, and its remaining validity time) when the remaining validity time of the key in use (encryption key/decryption key) reaches the first setting value (a value smaller than the initial value of the remaining validity time of the key in use and larger than 0), switches the key stored in the own table (the key information management table in the content server) to the new key to be used next when the remaining validity time of the key in use reaches 0, creates a new encryption key/decryption key to be used next and saves the key information (a set of the encryption key/decryption key, its key number, and its remaining validity time) in its own table;

an encryption/packet transmission means in the content server that encrypts the distributed data using the encryption key in use stored in its own table (the key information management table in the content server) at the time of multicast distribution, and transmits a multicast packet containing encrypted data and the key number of the encryption key;

10

a key information management table in the client that can store a pair of the decryption key in use, its key number, and its remaining validity time, and can store a pair of the decryption key to be used next, its key number, and its remaining validity time;

a packet receiving/decryption means in the client that receives multicast packets sent from the content server, searches for a decryption key from its own table (the key information management table in the client where it exists) based on the key number in the received multicast packet, and decrypts the encrypted data in the multicast packet using the decryption key of that key number;

a key management means in the client that transmits a key information request to the key management server when the remaining validity time of the key in use reaches the second setting value (a value smaller than the first setting value and larger than 0), saves a set of the decryption key to be used next, its key number, and its remaining validity time in the response message in the own table (the key information management table in the client where the self exists), and switches the key that was previously stored in the local table as the next key to be used to the new key in use based on recognition of changes in key numbers in multicast packets sent from the content server;

20

a key information management table in the key management server that can store a set of a decryption key in use, its key number, and its remaining validity time, and a set of a decryption key to be used next, its key number, and its remaining validity time; and

a key management means in the key management server that saves a set of the decryption key to be used next, its key number, and its remaining validity time in the key information message received from the content server in its own table (the key information management table in the key management server), transmits back a response message containing a set of the decryption key to be used next, its key number, and its remaining validity time to the client when receiving a key information request from the client when the remaining validity time of the key in use reaches the second setting value, and switches the key stored in the local table to the new key as the next key to be used when the remaining validity time of the key in use reaches 0.

[0014]

Here, the key exchange method in the multicast distribution system related to the present invention can be realized in a form that includes a content server key exchange control program for causing the content server to function as the key information management table, key management means, and encryption/packet transmission means, a client key management program for causing the client to function as the key information management table, packet receiving/decryption means, and key management means, and a key exchange control program for a key management server for causing the above key management server to function as the above key information management table and key management means.

30

[0015]

Further, the key exchange method in the multicast distribution system related to the present invention described above can be expressed, more generally, as comprising: a content server in which a network system where multicast distribution of encrypted data is performed creates an encryption key/decryption key, manages the encryption key/decryption key, its key number and remaining validity time, distributes the decryption key to be used next to the key management server within the validity time of the key in use (before the remaining validity time reaches 0), and transmits a multicast packet containing encrypted data and the key number of the encryption key used in the encryption; a client that requests the key management server to transmit the decryption key to be used next after the content server

40

50

distributes the decryption key to be used next to the key management server within the validity time of the key in use and decrypts the encrypted data in the multicast packet using the decryption key corresponding to the key number in the multicast packet received from the content server; and a key management server that manages the decryption key, its key number and remaining validity time, and receives the decryption key to be used next from the content server, and transmits the decryption key to be used next to the client in response to a request from the client.

[0016]

Further, the key exchange method in the multicast distribution system related to the present invention can be configured, in a network system where multicast distribution of encrypted data is performed, to comprise:

a key information management table in the content server that can hold a set of an encryption key in use, its key number, and its remaining validity time, and a set of an encryption key to be used next, its key number, and its remaining validity time; 10

a key management means in the content server that issues a key creation request to the key management server to request the creation of the next key to be used when the remaining validity time of the key in use reaches the first setting value (a value smaller than the initial value of the remaining validity time of the key in use and larger than 0), saves a set of the encryption key to be used next, its key number, and its remaining validity time in the key information response message received in its own table (the key information management table in the content server), and switches the key stored in the local table to the new key as the next key to be used when the remaining validity time of the key in use reaches 0;

an encryption/packet transmission means in the content server that encrypts the distributed data using the encryption key in use stored in its own table (the key information management table in the content server) at the time of multicast distribution, and transmits a multicast packet containing encrypted data and the key number of the encryption key;

a key information management table in the client that can store a pair of the decryption key in use, its key number, and its remaining validity time, and can store a pair of the decryption key to be used next, its key number, and its remaining validity time; 20

a packet receiving/decryption means in the client that receives multicast packets sent from the content server, searches for a decryption key from its own table (the key information management table in the client where it exists) based on the key number in the received multicast packet, and decrypts the encrypted data in the multicast packet using the decryption key of that key number;

a key management means in the client that transmits a key information request to the key management server when the remaining validity time of the key in use reaches the second setting value (a value smaller than the first setting value and larger than 0), saves a set of the decryption key to be used next, its key number, and its remaining validity time in the response message in its own table (the key information management table in the client where it exists), and switches the key that was previously stored in the local table as the next key to be used to the new key in use based on the recognition of changes in key numbers in multicast packets sent from content servers;

a key information management table in the key management server that can store a set of the encryption key/decryption key in use, its key number, and its remaining validity time, and can also store a set of the encryption key/decryption key to be used next, its key number, and its remaining validity time; and

a key management means in the key management server that creates the encryption key/decryption key to be used next in response to the key creation request received from the content server, saves a set of the encryption key/decryption key to be used next, its key number, and its remaining validity time in its own table (the key information management table in the key management server), returns a key information response message regarding the encryption key to be used next (a message having key information that is a set of the encryption key to be used next, its key number, and its remaining validity time) to the content server, returns a response message containing a set of the decryption key to be used next, its key number, and its remaining validity time to the client when receiving a key information request from the client when the remaining validity time of the key in use reaches the second setting value, and switches the key stored in the local table to the new key as the next key to be used when the remaining validity time of the key in use reaches 0. 30

[0017]

Here, the key exchange method in the multicast distribution system related to the present invention can be realized in a form that includes a content server key exchange control program for causing the content server to function as the key information management table, key management means, and encryption/packet transmission means, a client key management program for causing the client to function as the 40

40

50

key information management table, packet receiving/decryption means, and key management means, and a key exchange control program for a key management server for causing the above key management server to function as the above key information management table and key management means.

[0018]

Furthermore, the key exchange method in the multicast distribution system related to the present invention described above can, more generally, be expressed as having a network system where multicast distribution of encrypted data is performed, comprising: a client server that manages encryption keys, their key numbers, and remaining validity time, requests the key management server to create the next encryption key/decryption key within the validity time of the key in use, obtains the encryption key created in response to the request from the key management server, and transmits a multicast packet containing encrypted data and the key number of the encryption key used in the encryption; a client that requests the key management server to transmit the decryption key to be used next after the content server requests the key management server to create an encryption key/decryption key to be used next within the validity time of the key in use, and decrypts the encrypted data in the multicast packet using the decryption key corresponding to the key number in the multicast packet received from the content server; and the key management server that manages encryption keys, decryption keys, their key numbers and remaining validity time, creates and stores encryption keys and decryption keys to be used next in response to requests from the content server, transmits the encryption key to be used next to the content server, and transmits the decryption key to be used next to the client in response to a request from the client.

[0019]

Further, in the key exchange method in the multicast distribution system of the present invention as described above, by adding the address of the key management server to the information in the multicast packet transmitted from the content server to the client, it is possible to eliminate the need for the client to set the destination of the key information request (destination for querying and requesting the decryption key).

[0020]

[Embodiments of The Invention]

Next, the present invention will be described in detail with reference to the drawings.

[0021]

(1) First embodiment

[0022]

FIG. 1 is a block diagram showing the configuration of a key exchange method in a multicast distribution system according to a first embodiment of the present invention.

[0023]

With reference to FIG. 1, the key exchange method in the multicast distribution system according to this embodiment consists of: a content server 11 that transmits multicast packets; clients 51, 52,..., 5n (n is a positive integer) that receive multicast packets sent from the content server 11; a key management server 31 that stores the key information regarding the decryption key in the key information message 71 sent from the content server 11 and transmits a response message 82 in response to the key information request 81 from the client 5i (i is a positive integer from 1 to n); and a network 100 connecting the content server 11, the client 5i, and the key management server 31.

[0024]

The content server 11 has a key information management table 21 that stores pairs (key information) of keys (encryption keys and decryption keys) used to encrypt and decrypt data (distribution data) distributed by multicast packets, a key number for identifying the key, and the remaining validity time for the key (the key information management table can hold multiple pieces of key information). The encryption key and decryption key used in a pair of encryption and decryption processes may be the same or different depending on the encryption method, but in any case, they are identified by the same key number.

[0025]

Here, the key information management table 21 stores key information on the key currently in use and key information on the key to be

10

20

30

40

50

used next.

[0026]

The content server 11 includes a key management means 111 and an encryption and packet transmission means 112.

[0027]

The key management server 31 has a key information management table 41 that stores a pair (key information) of a key (in this embodiment, a decryption key), a key number for identifying that key, and the remaining validity time for that key.

[0028]

Here, the key information management table 41 stores key information relating to the key currently in use, and can also store key information relating to the key to be used next. In the initial state, the key information management table 41 does not contain any information.

[0029]

The key management server 31 includes a key management means 311.

[0030]

The client 5i has a key information management table 6i that stores a pair (key information) of a key (decryption key) used to decrypt data distributed by multicast packets, a key number for identifying the key, and the remaining validity time for the key.

[0031]

Here, the key information management table 6i stores key information on keys currently in use, and can also store key information on the key to be used next. In the initial state, the key information management table 6i does not contain any information.

[0032]

The client 5i includes a key management means 5i1 and a packet receiving and decrypting means 5i2.

[0033]

The content server 11, the key management server 31, and each client 5i update the remaining validity time in the key information in the key information management table 21, the key information management table 41, and each key information management table 6i that they manage every time the time passes (performing updates based on their own clock signals, and the like).

[0034]

FIG. 2 is a flow chart showing multicast packet transmission/reception processing using the key exchange method in the multicast distribution system according to this embodiment. This process comprises a distribution data encryption step A1, a multicast packet transmission step A2, a multicast packet receiving step A3, a currently used key number match determination step A4, a next key number match determination step A5, an encrypted data decryption step A6, and a key management server inquiry step A7.

[0035]

FIG. 3 is a flow chart showing processing relating to key management in the key exchange method in the multicast distribution system according to the present embodiment (processing performed when the remaining validity time of the key in use reaches the first setting value). This process comprises a first setting value reaching recognition step B1, a key information message transmitting step B2, a key information message receiving step B3, and a next use key information saving step B4.

[0036]

FIG. 4 is a flow chart showing processing relating to key management in the key exchange method in the multicast distribution system according to this embodiment (processing at the point in time when the remaining validity time of the key in use reaches the second setting value). This process comprises a second setting value reaching recognition step C1, a key information request transmitting step C2, a key information request receiving step C3, a response message transmitting step C4, a response message receiving step C5, and a next-use key information saving step C6.

[0037]

10

20

30

40

50

FIG. 5 is a block diagram for explaining a specific operation of the key exchange method in the multicast distribution system according to this embodiment.

[0038]

FIG. 6 is a sequence diagram for explaining a specific operation of the key exchange method in the multicast distribution system according to the present embodiment.

[0039]

Next, the overall operation of the key exchange method in the multicast distribution system according to the present embodiment configured as described above will be described in detail with reference to FIGS. 1 to 6.

[0040]

10

First, an operation relating to a multicast packet transmission/reception process performed from the content server 11 to each client 5i via the network 100 will be described (see FIG. 2).

[0041]

During multicast distribution, the encryption/packet transmission means 112 in the content server 11 encrypts the distribution data (data to be distributed) using the encryption key currently in use stored (the encryption key in the key information related to the key currently in use in the key information management table 21) (step A1).

[0042]

Further, a multicast packet containing the encrypted data (encrypted distribution data) and the key number of the encryption key is transmitted onto network 100 (step A2).

[0043]

The packet receiving and decrypting means 5i2 in the client 5i participating in the multicast address receives the multicast packet transmitted from the content server 11 (step A3), and performs a decryption process for the encrypted data contained in the received multicast packet.

20

[0044]

In this decryption process, first, the key number in the received multicast packet is compared with the key number of the decryption key currently in use stored in the device itself (the key number in the key information related to the key currently in use in the key information management table 6i) to determine whether the two key numbers match (step A4).

[0045]

If it is determined in step A4 that "the two key numbers match," the encrypted data in the multicast packet is decrypted using the decryption key of that key number (step A6).

[0046]

On the other hand, if it is determined in step A4 that the key numbers do not match, the device compares the key number in the multicast packet with the key number of the next decryption key to be used that is stored in the device itself (the key number in the key information related to the next key to be used in the key information management table 6i) to determine whether the key numbers match (step A5).

30

[0047]

If it is determined in step A5 that "the two key numbers match," the encrypted data in the multicast packet is decrypted using the decryption key of that key number (step A6).

[0048]

On the other hand, if it is determined in step A5 that "the two key numbers do not match" (including the case where there is no key information on the next key to be used in the key information management table 6i), that is, if the key numbers of both the key currently being used and the key to be used next do not match the key number in the multicast packet, the process of acquiring the key information has not been performed correctly, so an inquiry to that effect is made to the key management server 31 (step A7).

[0049]

Second, a description will be given of operations related to key management during the period when the remaining validity time of a key in use varies from the initial value (initial remaining validity time value) to a first setting value (a value smaller than the initial value).

40

[0050]

50

During this period, the key information management table 21 in the content server 11 stores key information (a set of a key, a key number, and the remaining validity time) regarding the keys (encryption key and decryption key) currently in use, and key information regarding the keys (encryption key and decryption key) to be used next. These keys and key numbers are created by the key management means 111 in the content server 11.

[0051]

During this period, the key information management table 41 in the key management server 31 stores key information relating to the key (decryption key) currently in use.

[0052]

Further, during this period, the key information management table 6i in each client 5i stores key information on the key (decryption key) currently in use (which is managed as key information for the next key to be used until a multicast packet including data encrypted by the key currently in use is received from the content server 11). Still further, until a multicast packet containing data encrypted with a new key in use is received from the content server 11, the key information relating to the key that was previously in use is also stored.

10

[0053]

If a client 5i newly joins the multicast address during this period, the key management unit 5i1 in the client 5i transmits a key information request 81 to the key management server 31. Then, the key management means 311 in the key management server 31 transmits a response message 82 containing key information relating to the key in use to the client 5i.

[0054]

Third, an operation relating to key management at the time when the remaining validity time of the key in use reaches the first setting value will be described (see FIG. 3).

[0055]

When the key management means 111 in the content server 11 recognizes that the remaining validity time of the key being used and managed in the key information management table 21 has reached the first setting value (the remaining validity time has decreased and reached the first setting value) (step B1), a message (key information message 71) containing key information (a set of key number, key, and remaining validity time) regarding the next key (decryption key) to be used is transmitted to the key management server 31 (step B2).

20

[0056]

When the key management means 311 in the key management server 31 receives the key information message 71 from the content server 11 (step B3), it stores the key information relating to the next key to be used in the key information message 71 in the key information management table 41 (step B4). As a result, the key information management table 41 in the key management server 31 stores key information on the key currently in use and key information on the key to be used next.

[0057]

If a client 5i newly joins the multicast address during the period from this point until the remaining validity time of the key in use reaches a second setting value (described later), the key management unit 5i1 in the client 5i transmits a key information request 81 to the key management server 31. Then, the key management means 311 in the key management server 31 transmits a response message 82 having key information on the key currently in use and key information on the key to be used next to the client 5i.

30

[0058]

Fourth, we will explain the operation related to key management when the remaining validity time of a key in use reaches a second setting value (a value smaller than the first setting value and greater than 0) (see FIG. 4).

[0059]

When the remaining validity time of the key in use in the key information management table 6i of the client 5i reaches the second setting value, the key management means 51 in the client 5i confirms to that effect (that the remaining validity time value has decreased and reached the second setting value) (step C1), and to obtain key information relating to the next key (decryption key) to be used, a key

40

50

information request 81 is sent to the key management server 31 (step C2). In addition, the address of the key management server 31 to which the key information request 81 is to be sent is preset in the client 5i.

[0060]

When the key management means 311 in the key management server 31 receives the key information request 81 from the client 5i (step C3), a response message 82 including key information on the key (decryption key) currently in use and key information on the key (decryption key) to be used next is transmitted to the client 5i (step C4) in response to the request.

[0061]

When the client 5i receives the response message 82 (step C5), it stores the key information relating to the next key to be used in the response message 82 in its own key information management table 6i (step C6).

[0062]

Fifth, the operation related to key management when the remaining validity time of a key in use reaches 0 will be described.

[0063]

When the remaining validity time of a key in use stored in the key information management table 21 becomes 0, the key management means 111 in the content server 11 discards the key information relating to the key currently in use, and saves the key information stored as the key information relating to the next key to be used in the key information management table 21 as the key information relating to the new key currently in use. As a result, the encryption/packet transmission means 112 uses that key to carry out subsequent encryption processing.

[0064]

At this time, the key management means 111 further creates new keys (encryption key and decryption key) to be used next, and stores in the key information management table 21 key information relating to the new keys to be used next.

[0065]

In addition, the encryption/packet transmission means 112 changes the key number contained in the encrypted packet (multicast packet having encrypted data) to the key number for the new key in use, thereby indicating to client 5i that the key in use has been changed.

[0066]

When the key management means 511 in each client 5i confirms that the key number included in the encrypted packet sent from the content server 11 (the encrypted packet received by the packet receiving/decrypting means 5i2) has been changed, it saves the next key to be used, which has the relevant key number in its own key information management table 6i, as the new key in use. At this time, each client 5i has not yet obtained a new key to be used next, and therefore does not have key information relating to the next key to be used in its own key information management table 6i.

[0067]

On the other hand, when the remaining validity time in the key information related to the key in use stored in the key information management table 41 becomes 0, the key management means 311 in the key management server 31 discards the key information relating to the key currently in use, and saves the key information stored as the key information relating to the next key to be used in the key information management table 41 as the key information relating to the new key currently in use. At this time, the key management server 31 has not yet obtained a new key to be used next, and therefore the key information management table 41 does not have key information relating to the next key to be used.

[0068]

The initial value of the remaining effective time, the first setting value (referred to as X) and the second setting value (referred to as Y) can be set, for example, as shown in the following method a or b.

[0069]

a. Manually set the common setting value for the entire multicast distribution system.

[0070]

b. The remaining validity time of the key and its initial value are transmitted to each device (key management server and client), and a certain percentage of the time from the initial value is calculated as X and Y in each device. This "certain percentage" is set

10

20

30

40

50

commonly throughout the entire multicast distribution system. As a specific example, if X is 50% of the initial value of the remaining validity time of the key and Y is 25% of the initial value of the remaining validity time of the key, X becomes 30 minutes and Y becomes 15 minutes, when the initial remaining validity time of the key is 1 hour.

[0071]

Next, a specific operation (series of operation sequences) of the key exchange method in the multicast distribution system according to this embodiment will be described with reference to FIG. 5 and FIG. 6.

[0072]

FIG. 5 is a diagram specifically showing the information in each key information management table and the contents of each packet/request/message. In FIG. 5, the key currently in use is indicated as key A, the next key to be used is indicated as key B, and their key numbers are indicated as "key number A" and "key number B." In this example, the encryption key and the decryption key are assumed to be the same key (for example, key A is both the encryption key and the decryption key). Further, the first setting value is indicated by X, and the second setting value is indicated by Y.

10

[0073]

FIG. 6 is a diagram showing an operation sequence over time when the information shown in FIG. 5 is handled.

[0074]

In this operation sequence, in the initial state (the state in which the remaining validity time value of key A is the initial value), the content server 11 has key information regarding key A, which is the key currently in use, and key B, which is the key to be used next. Further, the key management server 31 and the client 51 (here, the client 51 is the focus of attention among the multiple clients 51 to 5n) only have key information relating to the key A among the key information shown in FIG. 5. It is assumed that the initial value of the remaining validity time and the values of X and Y are set in advance in the content server 11, the key management server 31, and the clients 51 to 5n.

20

[0075]

When the remaining validity time of key A reaches X (first setting value), the content server 11 transmits a key information message 71 including key information on key B (the next key to be used) to the key management server 31. As a result, the key management server 31 has key information relating to the keys A and B, as shown in FIG. 5.

[0076]

When the remaining validity time of key A reaches Y (second setting value), the client 51 transmits a key information request 81 to the key management server 31, requesting key information on the next key to be used.

[0077]

In response to this key information request 81, the key management server 31 transmits a response message 82 having key information relating to the key currently in use (key A) and the next key to be used (key B). As a result, the client 51 has key information relating to the keys A and B, as shown in FIG. 5.

30

[0078]

When the remaining validity time value of key A becomes 0, the content server 11 discards key information on key A which is the key in use, stores key B which is the key to be used next and which has been saved, as the new key in use, and encrypts distribution data using key B. At this time, the content server 11 also generates a key C as a new key to be used next, and stores key information relating to this key C in the key information management table 21. This key information regarding key C is transmitted from content server 11 to key management server 31 in a key information message 71 when the remaining validity time of key B reaches X.

[0079]

When the remaining validity time of key A reaches 0, the key management server 31 discards the key information regarding key A and stores key B, which has been stored as the next key to be used, as the key currently in use. Further, when key information regarding key C is received from content server 11 via key information message 71, this key information is stored in key information management table

40

50

41 as key information regarding the key to be used next. As a result, the key information stored in the key information management table 41 will be such that the key information related to key A in Figure 5 is replaced with key information related to key B, and the key information related to key B in Figure 5 is replaced with key information related to key C.

[0080]

When client 51 receives a multicast packet having the key number of key B from content server 11, it discards the key information regarding key A and stores key B, which was saved as the key to be used next, as the key currently in use. Further, when the key management server 31 receives key information on the key C, which is the key to be used next after the key B, in a response message 82 from the key management server 31, the key management server 31 stores the key information in its own key information management table 6i. As a result, the key information stored in the key information management table 6i is such that the key information related to key A in FIG. 5 is replaced with key information related to key B, and the key information related to key B in Figure 5 is replaced with key information related to key C.

10

[0081]

By repeating the above operations, the client 51 (or, in general, each client 5i) can obtain key information regarding the next key to be used before the key is changed.

[0082]

In this embodiment, communication delays occurring in communications between the content server 11, the key management server 31, and the client 5i are not taken into consideration. Therefore, it is conceivable that a difference will occur in the remaining validity time values in the key information of the same key number in each of the key information management tables 21, 41, and 6i by the amount of such communication delay. Although it is unlikely that such a deviation will actually cause a problem, even if this is taken into consideration, appropriate measures can be taken as shown in a and b below.

[0083]

20

a. Even if encrypted data (a multicast packet having the encrypted data and the key number of the next key to be used) arrives using the key scheduled to be used next before the validity time of the key currently in use expires (before the remaining validity time becomes 0), because the client 5i has the above-mentioned configuration and operation, it stores key information regarding the next key to be used, thereby making it is possible to identify the key (decryption key) and making decryption possible using that decryption key.

[0084]

b. Even if encrypted data using an old key is sent after the validity time has expired, the client 5i will continue to use the old key even after the remaining validity time reaches 0. Until a multicast packet having the key number of the new key in use is received, the key information regarding the old key is stored, so that decryption using that key (decryption key) is possible.

[0085]

(2) Modification of the First Embodiment

[0086]

30

For the first embodiment described above, the following variations a and b can be considered with respect to the information contained in the multicast packet distributed from the content server 11 to the client 5i (a combination of a and b is also possible).

[0087]

a. In the first embodiment, the multicast packet includes encrypted data and a key number. Further, it is also possible to add the address of the key management server 31 (including information indicating the contact point, similar to the address). In this way, by adding the key management server address to the multicast packet and transmitting it, it is possible to eliminate the need for the client 5i to set the destination of the inquiry/request for key information (the destination of the key information request 81).

[0088]

b. It is also possible to add to a multicast packet the remaining validity time of the key identified by the key number contained in the multicast packet.

[0089]

40

50

7(3) Second Embodiment

[0090]

FIG. 7 is a block diagram showing the configuration of a key exchange method in a multicast distribution system according to the second embodiment of the present invention.

[0091]

With reference to FIG. 7, the key exchange method in the multicast distribution system according to this embodiment is configured to include: a content server 12 that transmits multicast packets; clients 51, 52,..., 5n (n is a positive integer) that receive multicast packets sent from the content server 12; a key management server 32 that creates and stores keys (encryption keys and decryption keys) in response to a key creation request 91 sent from the content server 12, returns a key information response message 92 having a set (key information) of the encryption key, a key number for identifying the key, and the remaining validity time of the key to the content server 12, and transmits a response message 82 in response to a key information request 81 from the client 5i (i is a positive integer from 1 to n); and a network 100 that connects the content server 12, client 5i, and key management server 32.

10

[0092]

The content server 12 has a key information management table 22 that stores a pair (key information) of a key (encryption key) used to encrypt data distributed by multicast packets, a key number for identifying the key, and the remaining validity time for the key (the key information management table can hold multiple pieces of key information).

[0093]

Here, the key information management table 22 stores key information relating to the key currently in use, and can also hold key information relating to the key to be used next.

[0094]

The content server 12 includes a key management means 121 and an encryption and packet transmission means 122.

20

[0095]

The key management server 32 has a key information management table 42 that stores a set (key information) of a key (encryption key/decryption key), a key number for identifying the key, and the remaining validity time for the key. In this embodiment, since the keys are created by the key management server 32, the key information management table 42 of the key management server 32 stores key information relating to encryption keys and decryption keys.

[0096]

Here, the key information management table 42 stores key information on the key currently in use and key information on the key to be used next.

[0097]

The key management server 32 includes a key management means 321.

[0098]

The client 5i has a key information management table 6i that stores a pair (key information) of a key (decryption key) used to decrypt data distributed by multicast packets, a key number for identifying the key, and the remaining validity time for the key.

30

[0099]

Here, the key information management table 6i stores key information on keys currently in use, and can also hold key information on the key to be used next. In the initial state, the key information management table 6i does not contain any information.

[0100]

The client 5i includes a key management means 5i1 and a packet receiving and decrypting means 5i2.

[0101]

The content server 12, the key management server 32, and each client 5i update the remaining validity times in the key information in the key information management table 22, the key information management table 42, and each key information management table 6i that they

40

50

manage every time the time passes (performing updates based on their own clock signals, and the like).

[0102]

The key exchange method in the multicast distribution system according to this embodiment, when compared to the first embodiment, is different in that the content server 12 transmits a key creation request 91 to the key management server 32, and in response, the key management server 32 creates a key (encryption key/decryption key) and returns a key information response message 92 containing key information regarding the created encryption key to the content server 12.

[0103]

FIG. 8 is a flow chart showing processing relating to key management in the key exchange method in the multicast distribution system according to this embodiment (processing at the point in time when the remaining validity time of the key in use reaches the first setting value). This process consists a first setting value arrival recognition step D1, a key creation request transmitting step D2, a key creation request receiving step D3, a next use key creation step D4, next use key information storage step D5, key information response message transmission step D6, key information response message reception step D7, and next use key information storage step D8.

10

[0104]

Next, with reference to FIGS. 7 and 8 (also with reference to FIGS. 1 to 4 as appropriate), the operation of the key exchange method in the multicast distribution system of this embodiment configured as described above will be described, focusing on the points that differ from the first embodiment.

[0105]

First, operations related to multicast packet transmission and reception processing performed from the content server 12 to each client 5i via the network 100 will be described.

[0106]

This operation is similar to the operation in the first embodiment (operation relating to multicast packet transmission and reception processing performed from the content server 11 in FIG. 1 to each client 5i via the network 100).

20

[0107]

Second, an operation relating to key management during the period when the remaining validity time of the key in use ranges from the initial value to a first setting value (a value smaller than the initial value) will be described.

[0108]

During this period, the key information management table 22 in the content server 12 stores key information (a set of a key, a key number, and a remaining validity time) relating to the key (encryption key) in use. These keys and key numbers are created by the key management means 321 in the key management server 32.

[0109]

During this period, the key information management table 42 in the key management server 32 stores key information (a set of a key, a key number, and a remaining validity time) relating to the keys (encryption keys and decryption keys) currently in use. These keys and key numbers are created by the key management means 321 in the key management server 32.

30

[0110]

Operations other than those described above are similar to those in the first embodiment.

[0111]

Third, an operation relating to key management when the remaining validity time of a key in use reaches the first setting value will be described (see FIG. 8).

[0112]

In the first embodiment, when the content server 11 recognizes that the remaining validity time of the key being used has reached the first setting value, the content server 11 transmits a key information message 71 to the key management server 31.

[0113]

In contrast, in this embodiment, when the key management means 121 in the content server 12 recognizes that the remaining validity time

40

50

of the key being used and managed in the key information management table 22 has reached the first setting value (a time point has been reached) (step D1), to obtain key information for the next key (encryption key) to be used, it transmits a key creation request 91 to the key management server 32 (step D2).

[0114]

When the key management means 321 in the key management server 32 receives the key creation request 91 from the content server 12 (step D3), it creates the next key to be used (encryption key/decryption key) in response to the key creation request 91 (step D4), and stores the key information for that key (a combination of the key, key number, and remaining validity time) in the key information management table 42 (step D5). As a result, the key information management table 42 in the key management server 32 stores key information relating to the key currently in use and key information relating to the next key to be used.

10

[0115]

Further, the key management means 321 transmits (returns) a key information response message 92 including key information (a set of the encryption key, key number, and remaining validity time) relating to the encryption key created in step D4 to the content server 12 (step D6).

[0116]

When the key management means 121 in the content server 12 receives the key information response message 92 from the key management server 32 (step D7), it stores the key information in the key information management table 22 regarding the next key (encryption key) to be used in the key information management table 22 (step D8). As a result, the key information management table 22 in the content server 12 stores key information relating to the key currently in use and key information relating to the key to be used next.

[0117]

Operations other than those described above are similar to those in the first embodiment.

[0118]

20

Fourth, an operation relating to key management when the remaining validity time of a key in use reaches a second setting value (a value smaller than the first setting value and larger than 0) will be described.

[0119]

This operation is similar to that in the first embodiment.

[0120]

Fifth, the operation related to key management when the remaining validity time of a key in use reaches 0 will be described.

[0121]

When the remaining validity time of a key in use stored in a key information management table 22 becomes 0, the key management means 121 in a content server 12 discards the key information on the key in use and stores the key information stored as the key information on the key to be used next in the key information management table 22 as the key information on a new key in use. At this time, the content server 12 has not yet obtained a new key to be used next, and therefore the key information management table 22 does not have key information relating to the next key to be used.

30

[0122]

As a result, the encryption/packet transmission means 122 uses that key (encryption key) to carry out subsequent encryption processing.

[0123]

Operations other than those described above are similar to those in the first embodiment.

[0124]

In the first embodiment described above, when a failure occurs in communication between the content server 11 and the key management server 31, it may become impossible to distribute the key (decryption key). In contrast, in this embodiment (second embodiment), even if a failure occurs in communication between the content server 12 and the key management server 32, it is possible to continue communication of multicast packets containing encrypted data by continuing to use the previous key.

[0125]

40

50

In this way, in the present invention, as shown in the first and second embodiments above, it is possible to realize a configuration in which the key is created by the content server, or a configuration in which the key is created by the key management server.

[0126]

(4) Modification of the Second Embodiment

[0127]

For the second embodiment, modifications similar to those for the first embodiment described in (2) a and b can be considered.

[0128]

(5) Third embodiment

[0129]

FIG. 9 is a block diagram showing the configuration of a key exchange method in a multicast distribution system according to the third embodiment of the present invention.

[0130]

Referring to FIG. 9, the key exchange method in the multicast distribution system according to the third embodiment of the present invention, when compared to the key exchange method in the multicast distribution system according to the first embodiment shown in FIG. 1, is different in that it comprises a content server key exchange control program 901, a key management server key exchange control program 902, and a client key exchange control program 903.

[0131]

The content server key exchange control program 901 is loaded into the content server 11 and controls the operation of the content server 11 as the key information management table 21, the key management means 111, and the encryption and packet transmission means 112. The operation of the content server 11 under the control of the content server key exchange control program 901 (operations relating to the key information management table 21, key management means 111, and encryption/packet transmission means 112) is exactly the same as the operation of the content server 11 in the first embodiment, and therefore a detailed explanation thereof will be omitted.

[0132]

Moreover, the key management server key exchange control program 902 is loaded into the key management server 31 and controls the operation of the key management server 31 as the key information management table 41 and the key management means 311. The operation of the key management server 31 under the control of the key exchange control program 902 for the key management server (operation relating to the key information management table 41 and the key management means 311) is exactly the same as the operation of the key management server 31 in the first embodiment, so detailed explanation thereof will be omitted.

[0133]

Further, the client key exchange control program 903 is loaded into each client 5i and controls the operation of each client 5i as a key information management table 6i, key management means 5i1, and packet receiving/decrypting means 5i2. The operation of each client 5i under the control of the client key exchange control program 903 (operation relating to the key information management table 6i, key management means 5i1, and packet receiving/decrypting means 5i2) is exactly the same as the operation of the client 5i in the first embodiment, so detailed explanations thereof will be omitted.

[0134]

(6) Fourth Embodiment

[0135]

FIG. 10 is a block diagram showing the configuration of a key exchange method in a multicast distribution system according to the fourth embodiment of the present invention.

[0136]

Referring to FIG. 10, the key exchange method in the multicast distribution system according to the fourth embodiment of the present invention is, when compared to the key exchange method in the multicast distribution system according to the second embodiment shown in FIG. 7, different in that it comprises a content server key exchange control program 1001, key management server key exchange control

10

20

30

40

50

program 1002, and client key exchange control program 1003.

[0137]

The content server key exchange control program 1001 is loaded into the content server 12 and controls the operation of the content server 12 as the key information management table 22, the key management means 121, and the encryption and packet transmission means 122. The operation of the content server 12 under the control of the content server key exchange control program 1001 (operations relating to the key information management table 22, the key management means 121, and the encryption and packet transmission means 122) is exactly the same as the operation of the content server 12 in the second embodiment, so a detailed explanation thereof will be omitted.

[0138]

Further, the key management server key exchange control program 1002 is loaded into the key management server 32 and controls the operation of the key management server 32 as the key information management table 42 and the key management means 321. The operation of the key management server 32 under the control of the key exchange control program 1002 for the key management server (operation relating to the key information management table 42 and the key management means 321) is exactly the same as the operation of the key management server 32 in the second embodiment, so detailed explanation thereof will be omitted.

10

[0139]

Further, the client key exchange control program 1003 is loaded into each client 5i and controls the operation of each client 5i as a key information management table 6i, key management means 5i1, and packet receiving/decrypting means 5i2. The operation of each client 5i under the control of the client key exchange control program 1003 (operation relating to the key information management table 6i, key management means 5i1, and packet receiving/decrypting means 5i2) is exactly the same as the operation of the client 5i in the second embodiment, so detailed explanations thereof will be omitted.

[0140]

[Effect of the Invention]

20

As described above, according to the present invention, the following effects are obtained.

[0141]

The first effect is that when a key is changed, no delay occurs for obtaining a new key. In other words, it is possible to change keys during multicast distribution without key exchange delay. The reason for this effect is that by managing key information, which includes the key number and the remaining validity time of the key along with the key itself, and allowing the client to obtain the next key to be used before the validity time of the key currently in use, decryption can be performed immediately using the new key when the key is replaced.

[0142]

A second effect is that it becomes unnecessary to set in a client the address of a key management server from which a key is requested when the client joins any multicast address. This effect occurs because the address of the key management server can be included in the multicast packet sent by the content server, and the client can make a key request to that key management server address.

[0143]

A third effect is that viewer (client) information can be obtained accurately in real time. The reason for this effect is by using the present invention, there is no delay when changing the key so the key change cycle can be shortened without increasing communication delay, and a cycle in which the client's information is aggregated by the key management server (a cycle in which the client's information is aggregated by the key management server when the client makes a key acquisition request to the key management server at predetermined intervals for decryption) can also be shortened and more accurate client information can be obtained.

30

[0144]

A fourth effect is that the advantage of the encryption method, that is, "the viewers (clients) are limited by encryption and unauthorized parties are prevented from obtaining information," can be more reliably realized. The reason for this effect is that, as described above, the

40

50

present invention can efficiently change the key at regular intervals, so that even if the key is leaked, unauthorized persons can be prevented from continuing to watch by changing the key. Also, by setting who is permitted or not permitted to view in a key management server that manages the key required for decryption, it is possible to specify who is to receive the decryption key.

[Brief Description of The Drawings]

FIG. 1 is a block diagram showing the configuration of a key exchange method in a multicast distribution system according to a first embodiment of the present invention.

FIG. 2 is a flowchart showing a multicast packet transmission/reception process using a key exchange method in the multicast distribution system shown in FIG. 1.

FIG. 3 is a flowchart showing processing relating to key management in the key exchange method in the multicast distribution system shown in FIG. 1 (processing at the time when the remaining validity time of the key in use reaches a first setting value). 10

FIG. 4 is a flowchart showing processing relating to key management in the key exchange method in the multicast distribution system shown in FIG. 1 (processing at the time when the remaining validity time of the key in use reaches a second setting value).

FIG. 5 is a block diagram for explaining a specific operation of a key exchange method in the multicast distribution system shown in FIG. 1.

FIG. 6 is a sequence diagram for explaining a specific operation of a key exchange method in the multicast distribution system shown in FIG. 1.

FIG. 7 is a block diagram showing the configuration of a key exchange method in a multicast distribution system according to a second embodiment of the present invention.

FIG. 8 is a flowchart showing processing relating to key management in the key exchange method in the multicast distribution system shown in FIG. 7 (processing at the time when the remaining validity time of the key in use reaches a first setting value).

FIG. 9 is a block diagram showing the configuration of a key exchange method in a multicast distribution system according to a third embodiment of the present invention. 20

FIG. 10 is a block diagram showing the configuration of a key exchange method in a multicast distribution system according to a fourth embodiment of the present invention.

[Explanation Of Symbols]

11, 12 content server

21, 22, 41, 42, 61, 62, ..., 6n key information management table

31, 32 key management server

51, 52, ..., 5n clients

71 key information message

81 key information request

82 response message

91 key creation request

92 key information response message

100 network

111, 121, 311, 321, 511, 521, ..., 5n1 key management means

112, 122 encryption and packet transmission means

512, 522, ..., 5n2 packet receiving and decryption means

901, 1001 content server key exchange control program

902, 1002 key management server key exchange control program

903, 1003 client key exchange control program

30

40

FIG. 1

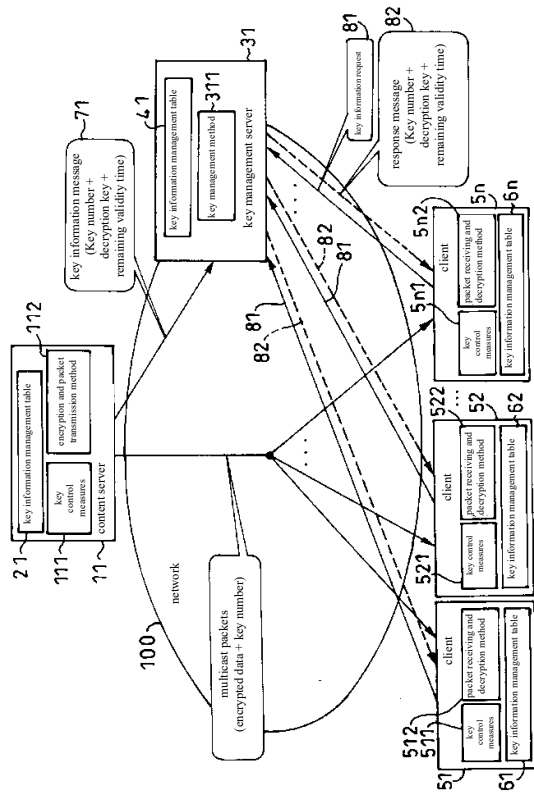


FIG. 2

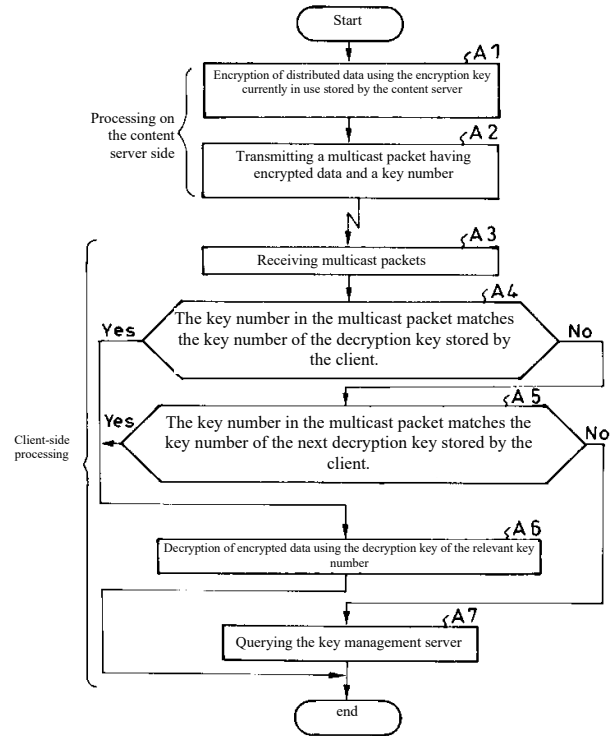


Figure 3

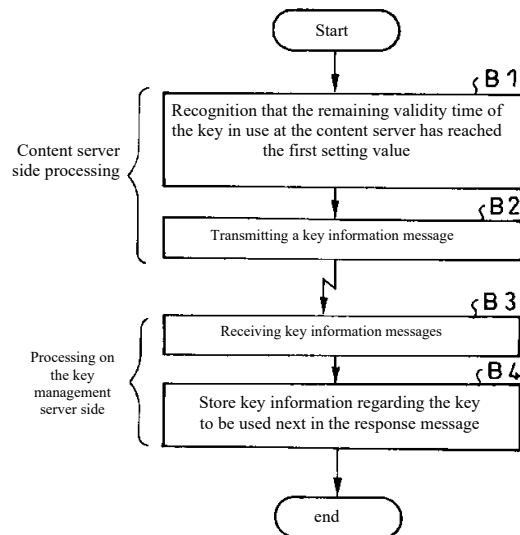


Figure 4

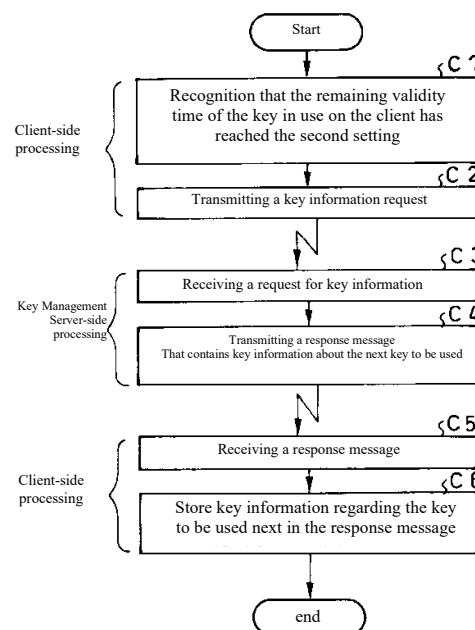


Figure 5

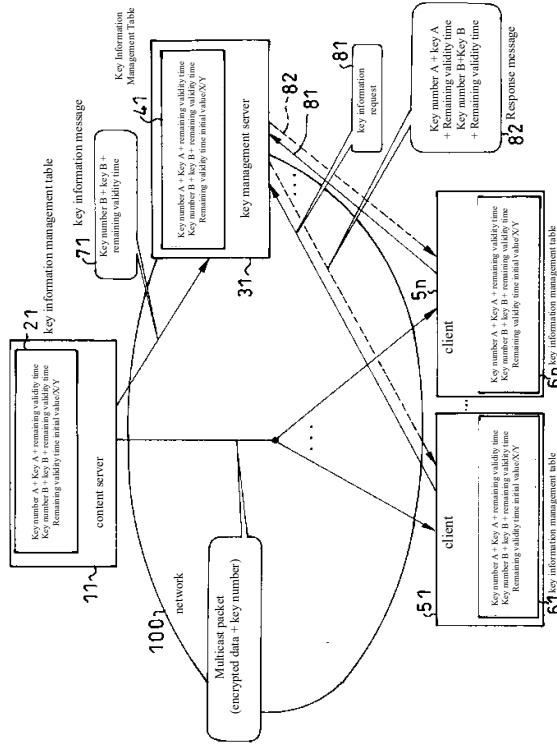


Figure 7

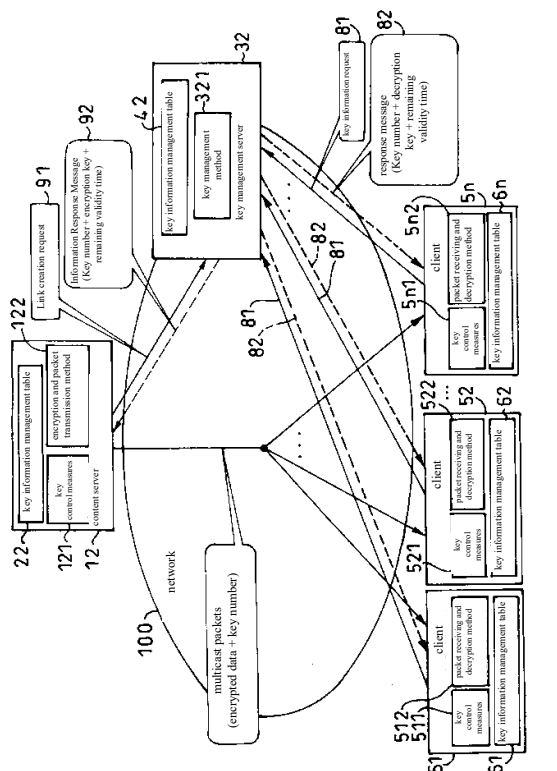


Figure 6

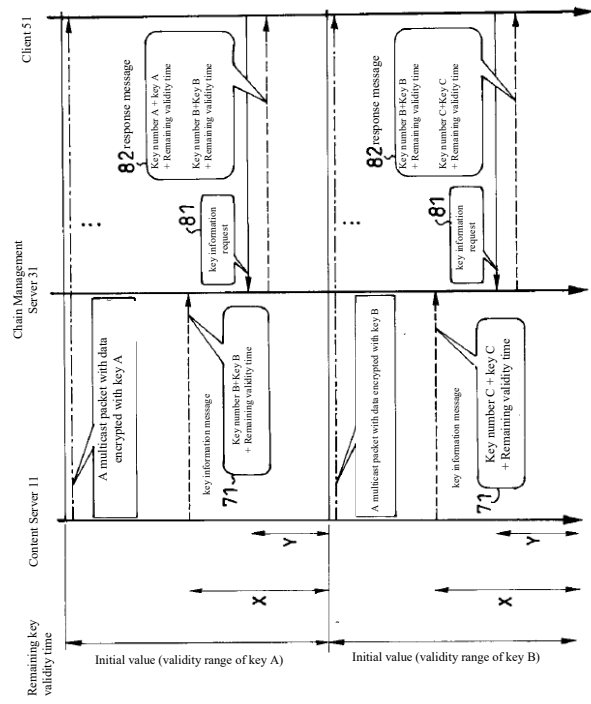


Figure 8

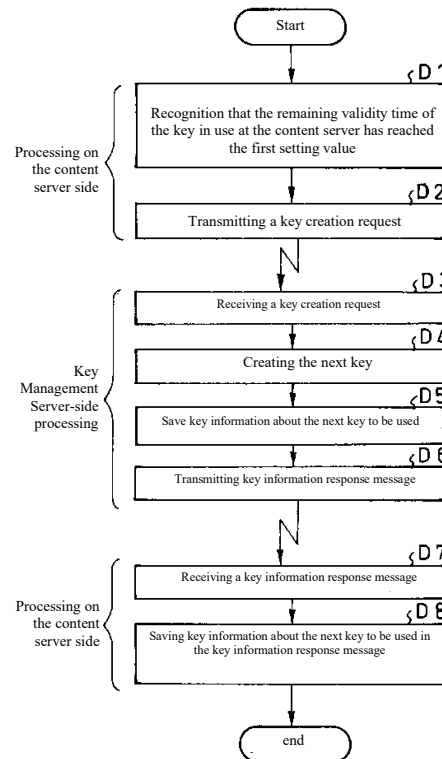


Figure 9

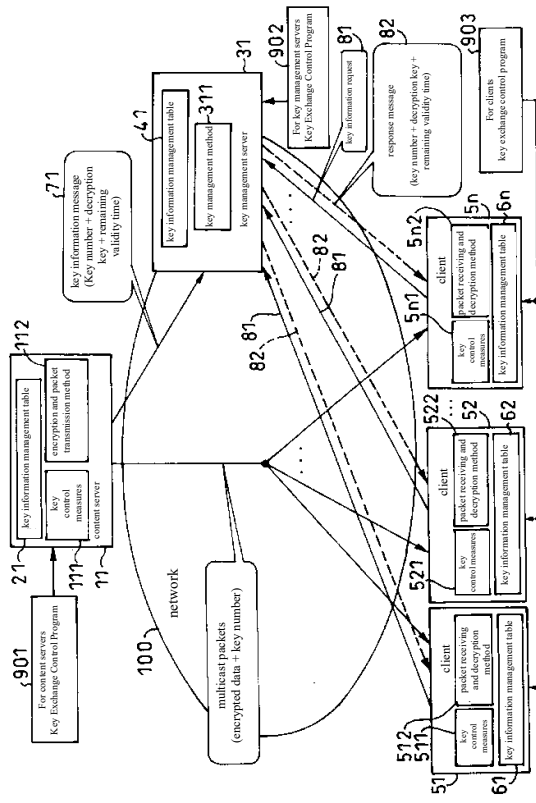
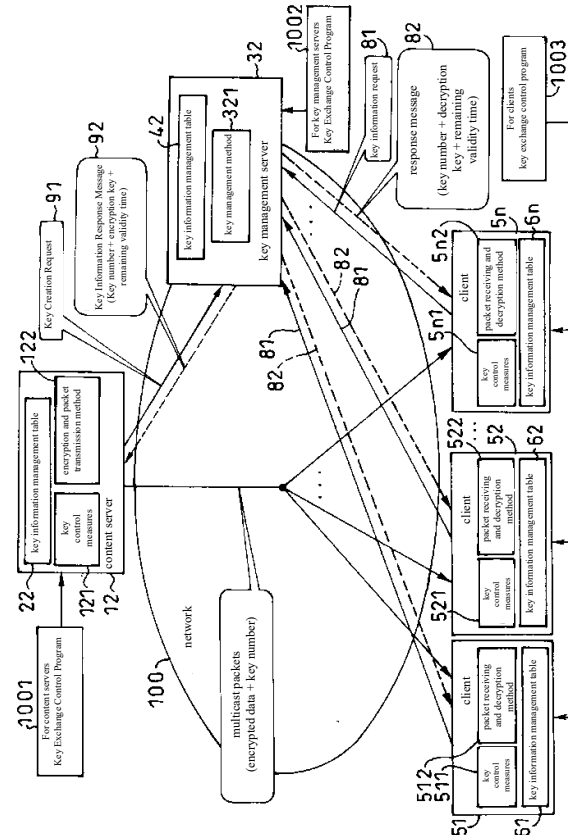


Figure 10



Front page continued

(72) Inventor: Hideyuki Magoe

Nippon Electric Communication Systems Co., Ltd. 1-4-28 Mita, Minato-ku, Tokyo

F-term (reference) 5J104 AA16 AA34 BA03 EA01 EA04 EA18 JA03 MA05 NA02 PA05
PA07

(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2004-166153

(P2004-166153A)

(43) 公開日 平成16年6月10日(2004.6.10)

(51) Int. Cl.⁷

H04L 9/08

H04L 9/14

F I

H04L 9/00

601B

H04L 9/00

641

テーマコード (参考)

5J104

審査請求 有 請求項の数 8 O L (全 25 頁)

(21) 出願番号 特願2002-332404 (P2002-332404)

(22) 出願日 平成14年11月15日 (2002.11.15)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(71) 出願人 000232254

日本電気通信システム株式会社

東京都港区三田1丁目4番28号

(74) 代理人 100088890

弁理士 河原 純一

(72) 発明者 鈴木 一哉

東京都港区芝五丁目7番1号 日本電気株式会社内

(72) 発明者 地引 昌弘

東京都港区芝五丁目7番1号 日本電気株式会社内

最終頁に続く

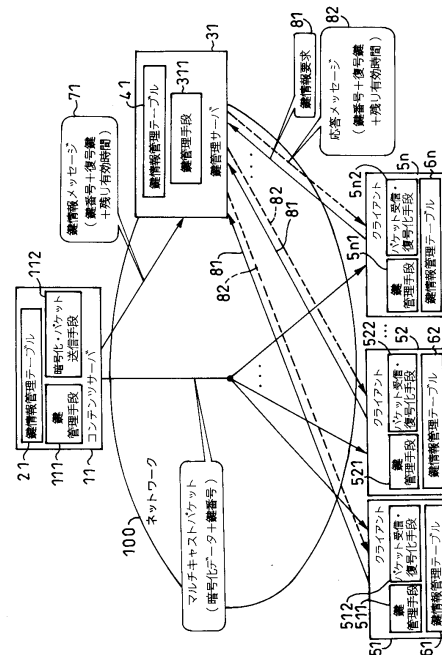
(54) 【発明の名称】 マルチキャスト配信システムにおける鍵交換方式

(57) 【要約】

【課題】 鍵変更（交換）時に、新しい復号鍵をクライアントが取得するために生じる処理の遅延を回避する。

【解決手段】 コンテンツサーバ11は、使用中の鍵の有効時間内に次に使用する復号鍵を鍵管理サーバ31に配布し、鍵番号を含むマルチキャストパケットを送信する。各クライアント51～5nは、使用中の鍵の有効時間内であってコンテンツサーバ11が鍵管理サーバ31に次に使用する復号鍵を配布した後の時点に、鍵管理サーバ31に対して当該次に使用する復号鍵の送付を要求する。また、マルチキャストパケット中の鍵番号に対応する復号鍵により当該マルチキャストパケット中の暗号化データの復号化を行う。鍵管理サーバ31は、コンテンツサーバ11から次に使用する復号鍵を受け取り、各クライアント51～5nからの送付要求に応じて当該次に使用する復号鍵をその要求元に送信する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵を作成し、当該暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内に次に使用する復号鍵を鍵管理サーバに配布し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、

使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する復号鍵を配布した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、

復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバから次に使用する復号鍵を受け取り、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項 2】

暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内に次に使用する暗号鍵・復号鍵の作成を鍵管理サーバに要求し、その要求に応じて作成された暗号鍵を前記鍵管理サーバから取得し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、

使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する暗号鍵・復号鍵の作成を要求した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、

暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバからの要求に応じて次に使用する暗号鍵・復号鍵を作成・保管し、当該次に使用する暗号鍵を前記コンテンツサーバに送信し、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項 3】

コンテンツサーバからクライアントに送信されるマルチキャストパケット中の情報に鍵管理サーバのアドレスを加えることによって、クライアント側での復号鍵の間合せ・要求先の設定を不要にすることを特徴とする請求項 1 または請求項 2 記載のマルチキャスト配信システムにおける鍵交換方式。

【請求項 4】

暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組および次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持するコンテンツサーバ内の鍵情報管理テーブルと、

使用中の鍵の残り有効時間が第 1 設定値となった時に、鍵管理サーバに対して次に使用する復号鍵に関する鍵情報メッセージを送信し、使用中の鍵の残り有効時間が 0 となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えて、新たな次に使用する暗号鍵・復号鍵を作成してその鍵情報を自テーブルに保存するコンテンツサーバ内の鍵管理手段と、

マルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、

10

20

30

40

50

使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、

コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、

使用中の鍵の残り有効時間が第2設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、

コンテンツサーバから受け取った鍵情報メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段とを有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項5】

暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

使用中の暗号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵とその鍵番号とその残り有効時間との組を保持しうるコンテンツサーバ内の鍵情報管理テーブルと、

使用中の鍵の残り有効時間が第1設定値となった時に、鍵管理サーバに対して次に使用する鍵の作成を要求する鍵作成要求を発行し、その応答として受け取る鍵情報応答メッセージ中の次に使用する暗号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えるコンテンツサーバ内の鍵管理手段と、マルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、

使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、

コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、

使用中の鍵の残り有効時間が第2設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、

10

20

30

40

50

コンテンツサーバから受け取った鍵作成要求に応じて、次に使用する暗号鍵・復号鍵を作成し、当該次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、当該次に使用する暗号鍵に関する鍵情報応答メッセージをコンテンツサーバに返送し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段と
を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項6】

コンテンツサーバからクライアントに送信されるマルチキャストパケット中の情報に鍵管理サーバのアドレスを加えることによって、クライアント側での鍵情報要求の送信先の設定を不要にすることを特徴とする請求項4または請求項5記載のマルチキャスト配信システムにおける鍵交換方式。

【請求項7】

暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、コンテンツサーバを、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組および次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持する鍵情報管理テーブル、使用中の鍵の残り有効時間が第1設定値となった時に、鍵管理サーバに対して次に使用する復号鍵に関する鍵情報メッセージを送信し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えて、新たな次に使用する暗号鍵・復号鍵を作成してその鍵情報を自テーブルに保存する鍵管理手段、ならびにマルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信する暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、

クライアントを、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持する鍵情報管理テーブル、コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うパケット受信・復号化手段、および使用中の鍵の残り有効時間が第2設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるためのクライアント用鍵交換制御プログラムと、

鍵管理サーバを、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持する鍵情報管理テーブル、およびコンテンツサーバから受け取った鍵情報メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【請求項8】

暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、コンテンツサーバを、使用中の暗号鍵とその鍵番号とその残り有効時間との組を保持し、

10

20

30

40

50

次に使用する暗号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル、使用中の鍵の残り有効時間が第1設定値となった時に、鍵管理サーバに対して次に使用する鍵の作成を要求する鍵作成要求を発行し、その応答として受け取る鍵情報応答メッセージ中の次に使用する暗号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理手段、およびマルチキャスト配信時に自テーブルに保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信する暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、クライアントを、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル、コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブルから復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うパケット受信・復号化手段、および使用中の鍵の残り有効時間が第2設定値となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるためのクライアント用鍵交換制御プログラムと、

鍵管理サーバを、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵情報管理テーブル、およびコンテンツサーバから受け取った鍵作成要求に応じて、次に使用する暗号鍵・復号鍵を作成し、当該次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を自テーブルに保存し、当該次に使用する暗号鍵に関する鍵情報応答メッセージをコンテンツサーバに返送し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムと

を有することを特徴とするマルチキャスト配信システムにおける鍵交換方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、マルチキャスト配信時に一定時間毎に異なる鍵によって暗号化を行うことで盗聴を防ぐマルチキャスト配信システムに関し、鍵（暗号鍵／復号鍵）の交換を制御・管理するためのマルチキャスト配信システムにおける鍵交換方式に関する。

【0002】

【従来の技術】

一般に、マルチキャストのパケットは不特定多数の受信者によって受信されるので、特定のクライアントのみに視聴を許可するためには、当該パケットによって配信されるデータに対して暗号鍵による暗号化を施し、視聴を許可したクライアントにのみ復号鍵を配布する必要がある。

【0003】

このとき、定期的に鍵を変更することで、クライアントを管理し、さらに暗号の秘匿性を向上させることができる。

【0004】

従来より、配信データ（配信対象のデータ）の暗号化が行われるマルチキャスト配信システムにおいては、一定時間毎に異なる鍵によって暗号化を行うことで盗聴を防ぐために、

10

20

30

40

50

暗号鍵や復号鍵の交換が行われていた（例えば、特許文献 1 参照）。

【 0 0 0 5 】

このような従来のマルチキャスト配信システムは、コンテンツサーバ（特許文献 1 では「送信部」と表現されている）とクライアント（特許文献 1 では「受信部」と表現されている）と鍵管理サーバとを含んで構成されており、コンテンツサーバが一定時間毎に鍵要求情報を添付したパケットを送信し、それを受けたクライアントが鍵管理サーバに対して鍵を要求することで、一定時間毎に鍵を更新し、鍵が第三者に渡った際にも暗号化データが流出することを防いでいる。

【 0 0 0 6 】

【特許文献 1】

特開 2 0 0 1 - 2 8 5 2 7 3 号公報（第 2 - 4 頁、図 1）

【 0 0 0 7 】

【発明が解決しようとする課題】

上述した従来のマルチキャスト配信システムにおける鍵交換方式には、次のような問題点があった。

【 0 0 0 8 】

第 1 の問題点は、鍵要求情報の受信時にタイムラグが生じるという点である。このような問題点が存在する理由は、クライアントが鍵要求情報を受け取った際に、鍵管理サーバに対して鍵を要求しその要求の応答（鍵）を受けてから復号化を開始するため、鍵管理サーバから応答が帰ってくるまでクライアントは暗号化情報（暗号化データ）の復号化ができないからである。

【 0 0 0 9 】

第 2 の問題点は、放送途中にマルチキャスト放送に参加した場合は即時に視聴することができないという点である。このような問題点が存在する理由は、鍵要求情報が添付されたパケットは一定間隔毎に発生するものであるため、マルチキャスト放送に参加したクライアントは次の鍵要求情報が送られてくるまで復号鍵を取得できず、復号化ができないからである。

【 0 0 1 0 】

第 3 の問題点は、マルチキャスト配信した鍵要求情報が経路上で消失した際に鍵の取得ができない期間が長期になるおそれがあるという点である。このような問題点が存在する理由は、マルチキャスト配信は応答確認が行われなため、経路上でパケットが消失したことが確認できないので、鍵要求情報を添付したパケットが消失した場合に、次の鍵要求情報が送られてくるまで新しい鍵の取得ができないからである。したがって、新しい鍵が取得できるまで、暗号化情報の復号化ができないようになる。

【 0 0 1 1 】

本発明の目的は、上述の点に鑑み、以上の問題点を解決し、マルチキャスト配信時に一定時間毎に異なる鍵によって暗号化を行うことで盗聴を防ぐネットワークシステムにおいて、鍵の変更（交換）時の確認遅延（鍵交換遅延）をなくしてリアルタイムのデータの処理を可能にするマルチキャスト配信システムにおける鍵交換方式を提供することにある。

【 0 0 1 2 】

すなわち、本発明の特徴は、マルチキャスト配信時に配信データを暗号化する場合に、暗号鍵・復号鍵を定期的に変更することによって暗号の秘匿性を向上し、かつ、鍵変更時の新しい鍵情報（鍵およびそれに付随する情報）の取得（クライアントによる取得）に伴う遅延を防ぐことを可能にする点にある。

【 0 0 1 3 】

【課題を解決するための手段】

本発明のマルチキャスト配信システムにおける鍵交換方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、使用中の暗号鍵・復号鍵（対となる暗号鍵および復号鍵。同じ鍵である場合もある）とその鍵番号（その鍵を識別するための情報）とその残り有効時間との組（その鍵に関する鍵情報）および次に使用する暗号鍵・

10

20

30

40

50

復号鍵とその鍵番号とその残り有効時間との組を保持するコンテンツサーバ内の鍵情報管理テーブルと、使用中の鍵（暗号鍵・復号鍵）の残り有効時間が第1設定値（使用中の鍵の残り有効時間の初期値よりも小さい値であり0よりも大きい値）となった時に、鍵管理サーバに対して次に使用する復号鍵に関する鍵情報メッセージ（次に使用する復号鍵とその鍵番号とその残り有効時間との組である鍵情報を有するメッセージ）を送信し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保持されていた鍵を新しい使用中の鍵に切り替えて、新たな次に使用する暗号鍵・復号鍵を作成してその鍵情報（当該暗号鍵・復号鍵とその鍵番号とその残り有効時間との組）を自テーブルに保存するコンテンツサーバ内の鍵管理手段と、マルチキャスト配信時に自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）から復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、使用中の鍵の残り有効時間が第2設定値（第1設定値よりも小さい値であり0よりも大きい値）となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）に保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、コンテンツサーバから受け取った鍵情報メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブル（鍵管理サーバ内の前記鍵情報管理テーブル）に保存し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段とを有する。

10

20

30

【0014】

ここで、本発明のマルチキャスト配信システムにおける鍵交換方式は、上記のコンテンツサーバを、上記の鍵情報管理テーブル、鍵管理手段、および暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、上記のクライアントを、上記の鍵情報管理テーブル、パケット受信・復号化手段、および鍵管理手段として機能させるためのクライアント用鍵管理プログラムと、上記の鍵管理サーバを、上記の鍵情報管理テーブルおよび鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムとを有する態様で実現することも可能である。

40

【0015】

なお、上記の本発明のマルチキャスト配信システムにおける鍵交換方式は、より一般的には、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵を作成し、当該暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内（残り有効時間が0となる前）に次に使用する復号鍵を鍵管理サーバに配布し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する復号鍵を配布した後の時点に前記鍵

50

管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバから次に使用する復号鍵を受け取り、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバとを有すると表現することができる。

【0016】

また、本発明のマルチキャスト配信システムにおける鍵交換方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、使用中の暗号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵とその鍵番号とその残り有効時間との組を保持しうるコンテンツサーバ内の鍵情報管理テーブルと、使用中の鍵の残り有効時間が第1設定値（使用中の鍵の残り有効時間の初期値よりも小さい値であり0よりも大きい値）となった時に、鍵管理サーバに対して次に使用する鍵の作成を要求する鍵作成要求を発行し、その応答として受け取る鍵情報応答メッセージ中の次に使用する暗号鍵とその鍵番号とその残り有効時間との組を自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保存し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替えるコンテンツサーバ内の鍵管理手段と、マルチキャスト配信時に自テーブル（コンテンツサーバ内の前記鍵情報管理テーブル）に保持されている使用中の暗号鍵を用いて配信データを暗号化し、暗号化データと当該暗号鍵の鍵番号とを有するマルチキャストパケットを送信するコンテンツサーバ内の暗号化・パケット送信手段と、使用中の復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する復号鍵とその鍵番号とその残り有効時間との組を保持しうるクライアント内の鍵情報管理テーブルと、コンテンツサーバから送信されてきたマルチキャストパケットを受信し、受信したマルチキャストパケット中の鍵番号によって自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）から復号鍵を検索し、その鍵番号の復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内のパケット受信・復号化手段と、使用中の鍵の残り有効時間が第2設定値（第1設定値よりも小さい値であり0よりも大きい値）となった時に、鍵管理サーバに対して鍵情報要求を送信し、その返信である応答メッセージ中の次に使用する復号鍵とその鍵番号とその残り有効時間との組を自テーブル（自己が存在するクライアント内の前記鍵情報管理テーブル）に保存し、コンテンツサーバから送信されてくるマルチキャストパケット中の鍵番号の変化の認識に基づいてそれまで次に使用する鍵として自テーブルに保持していた鍵を新しい使用中の鍵に切り替えるクライアント内の鍵管理手段と、使用中の暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持し、次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を保持しうる鍵管理サーバ内の鍵情報管理テーブルと、コンテンツサーバから受け取った鍵作成要求に応じて、次に使用する暗号鍵・復号鍵を作成し、当該次に使用する暗号鍵・復号鍵とその鍵番号とその残り有効時間との組を自テーブル（鍵管理サーバ内の前記鍵情報管理テーブル）に保存し、当該次に使用する暗号鍵に関する鍵情報応答メッセージ（当該次に使用する暗号鍵とその鍵番号とその残り有効時間との組である鍵情報を有するメッセージ）をコンテンツサーバに返送し、使用中の鍵の残り有効時間が第2設定値となった時にクライアントから鍵情報要求を受け取った際に、次に使用する復号鍵とその鍵番号とその残り有効時間との組を含む応答メッセージを当該クライアントに返送し、使用中の鍵の残り有効時間が0となった時に、次に使用する鍵として自テーブルに保持されていた鍵を新しい使用中の鍵に切り替える鍵管理サーバ内の鍵管理手段とを有するように構成することも可能である。

【0017】

ここで、本発明のマルチキャスト配信システムにおける鍵交換方式は、上記のコンテンツサーバを、上記の鍵情報管理テーブル、鍵管理手段、および暗号化・パケット送信手段として機能させるためのコンテンツサーバ用鍵交換制御プログラムと、上記のクライアントを、上記の鍵情報管理テーブル、パケット受信・復号化手段、および鍵管理手段として機

10

20

30

40

50

能させるためのクライアント用鍵管理プログラムと、上記の鍵管理サーバを、上記の鍵情報管理テーブルおよび鍵管理手段として機能させるための鍵管理サーバ用鍵交換制御プログラムとを有する態様で実現することも可能である。

【0018】

なお、上記の本発明のマルチキャスト配信システムにおける鍵交換方式は、より一般的には、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵とその鍵番号および残り有効時間とを管理し、使用中の鍵の有効時間内に次に使用する暗号鍵・復号鍵の作成を鍵管理サーバに要求し、その要求に応じて作成された暗号鍵を前記鍵管理サーバから取得し、暗号化データとその暗号化で使用した暗号鍵の鍵番号とを有するマルチキャストパケットの送信を行うコンテンツサーバと、使用中の鍵の有効時間内であって前記コンテンツサーバが前記鍵管理サーバに次に使用する暗号鍵・復号鍵の作成を要求した後の時点に前記鍵管理サーバに対して当該次に使用する復号鍵の送付を要求し、前記コンテンツサーバから受信したマルチキャストパケット中の鍵番号に対応する復号鍵によって当該マルチキャストパケット中の暗号化データの復号化を行うクライアントと、暗号鍵・復号鍵とその鍵番号および残り有効時間とを管理し、前記コンテンツサーバからの要求に応じて次に使用する暗号鍵・復号鍵を作成・保管し、当該次に使用する暗号鍵を前記コンテンツサーバに送信し、前記クライアントからの要求に応じて当該次に使用する復号鍵を前記クライアントに送信する前記鍵管理サーバとを有すると表現することができる。

10

【0019】

さらに、以上列举した本発明のマルチキャスト配信システムにおける鍵交換方式においては、コンテンツサーバからクライアントに送信されるマルチキャストパケット中の情報に鍵管理サーバのアドレスを加えることによって、クライアント側での鍵情報要求の送信先（復号鍵の問合せ・要求先）の設定を不要にすることも可能である。

20

【0020】

【発明の実施の形態】

次に、本発明について図面を参照して詳細に説明する。

【0021】

(1) 第1の実施の形態

【0022】

図1は、本発明の第1の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

30

【0023】

図1を参照すると、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、マルチキャストパケットを送信するコンテンツサーバ11と、コンテンツサーバ11より送られたマルチキャストパケットを受信するクライアント51, 52, ..., 5n (nは正整数)と、コンテンツサーバ11から送られた鍵情報メッセージ71中の復号鍵に関する鍵情報を保管しクライアント5i (iは1~nの正整数)からの鍵情報要求81に対して応答メッセージ82を送信する鍵管理サーバ31と、コンテンツサーバ11, クライアント5i, および鍵管理サーバ31を接続するネットワーク100とを含んで構成されている。

40

【0024】

コンテンツサーバ11は、マルチキャストパケットによって配信されるデータ（配信データ）の暗号化・復号化に用いる鍵（暗号鍵・復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル21を有する（鍵情報管理テーブルは鍵情報を複数保持しうる）。なお、一対の暗号化・復号化処理で用いられる暗号鍵と復号鍵とは、暗号化方式によって、同一である場合も異なる場合もあるが、いずれにしても同一の鍵番号によって識別される。

【0025】

ここで、鍵情報管理テーブル21は、使用中の鍵に関する鍵情報と、次に使用する鍵に関

50

する鍵情報とを保持している。

【0026】

また、コンテンツサーバ11は、鍵管理手段111と、暗号化・パケット送信手段112とを含んで構成されている。

【0027】

鍵管理サーバ31は、鍵（本実施の形態では、復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル41を有する。

【0028】

ここで、鍵情報管理テーブル41は、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。なお、初期状態では、鍵情報管理テーブル41は情報を持っていない。

10

【0029】

また、鍵管理サーバ31は、鍵管理手段311を含んで構成されている。

【0030】

クライアント5iは、マルチキャストパケットによって配信されるデータの復号化に用いる鍵（復号鍵）とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組（鍵情報）を保持する鍵情報管理テーブル6iを有する。

【0031】

ここで、鍵情報管理テーブル6iは、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。なお、初期状態では、鍵情報管理テーブル6iは情報を持っていない。

20

【0032】

また、クライアント5iは、鍵管理手段5i1と、パケット受信・復号化手段5i2とを含んで構成されている。

【0033】

なお、コンテンツサーバ11、鍵管理サーバ31、および各クライアント5iは、それぞれの管理する鍵情報管理テーブル21、鍵情報管理テーブル41、および各鍵情報管理テーブル6i上の鍵情報中の残り有効時間を時間の経過毎に更新する（自己のクロック信号に基づく更新等を行う）。

30

【0034】

図2は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式のマルチキャストパケット送受信処理を示す流れ図である。この処理は、配信データ暗号化ステップA1と、マルチキャストパケット送信ステップA2と、マルチキャストパケット受信ステップA3と、使用中鍵番号一致判定ステップA4と、次使用鍵番号一致判定ステップA5と、暗号化データ復号化ステップA6と、鍵管理サーバ問い合わせステップA7とからなる。

【0035】

図3は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第1設定値となった時点における処理）を示す流れ図である。この処理は、第1設定値到達認識ステップB1と、鍵情報メッセージ送信ステップB2と、鍵情報メッセージ受信ステップB3と、次使用鍵情報保存ステップB4とからなる。

40

【0036】

図4は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第2設定値となった時点における処理）を示す流れ図である。この処理は、第2設定値到達認識ステップC1と、鍵情報要求送信ステップC2と、鍵情報要求受信ステップC3と、応答メッセージ送信ステップC4と、応答メッセージ受信ステップC5と、次使用鍵情報保存ステップC6とからなる。

【0037】

50

図5は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのブロック図である。

【0038】

図6は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのシーケンス図である。

【0039】

次に、図1～図6を参照して、上記のように構成された本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の全体の動作について詳細に説明する。

【0040】

第1に、コンテンツサーバ11から各クライアント5iにネットワーク100を介して行われるマルチキャストパケット送受信処理に関する動作について説明する（図2参照）。 10

【0041】

コンテンツサーバ11内の暗号化・パケット送信手段112は、マルチキャスト配信時に、自身が保持している現在使用中の暗号鍵（鍵情報管理テーブル21内の使用中の鍵に関する鍵情報中の暗号鍵）を用いて、配信データ（配信対象のデータ）の暗号化を行う（ステップA1）。

【0042】

その上で、暗号化データ（暗号化された配信データ）と当該暗号鍵の鍵番号とを有するマルチキャストパケットをネットワーク100上に送信する（ステップA2）。 20

【0043】

マルチキャストアドレスに参加しているクライアント5i内のパケット受信・復号化手段5i2は、コンテンツサーバ11から送信されたマルチキャストパケットを受信し（ステップA3）、受信したマルチキャストパケットに含まれている暗号化データの復号化処理を行う。

【0044】

この復号化処理に際しては、まず、受信したマルチキャストパケット中の鍵番号と自身が記憶している現在使用中の復号鍵の鍵番号（鍵情報管理テーブル6i内の使用中の鍵に関する鍵情報中の鍵番号）とを比較し、両鍵番号が一致するか否かを判定する（ステップA4）。 30

【0045】

ステップA4で「両鍵番号が一致する」と判定した場合には、当該鍵番号の復号鍵を利用して当該マルチキャストパケット中の暗号化データの復号化を行う（ステップA6）。 40

【0046】

一方、ステップA4で「両鍵番号が一致しない」と判定した場合には、当該マルチキャストパケット中の鍵番号と自身が記憶している次に使用する復号鍵の鍵番号（鍵情報管理テーブル6i内の次に使用する鍵に関する鍵情報中の鍵番号）とを比較し、両鍵番号が一致するか否かを判定する（ステップA5）。

【0047】

ステップA5で「両鍵番号が一致する」と判定した場合には、当該鍵番号の復号鍵を利用して当該マルチキャストパケット中の暗号化データの復号化を行う（ステップA6）。 40

【0048】

一方、ステップA5で「両鍵番号が一致しない」と判定した場合（鍵情報管理テーブル6i内に次に使用する鍵に関する鍵情報が存在しない場合を含む）、すなわち、使用中の鍵および次に使用する鍵のどちらの鍵番号についても当該マルチキャストパケット中の鍵番号とは一致しなかった場合には、鍵情報の取得処理が正しく行われていないことを意味するため、鍵管理サーバ31にその旨の問い合わせを行う（ステップA7）。

【0049】

第2に、使用中の鍵の残り有効時間の値が初期値（残り有効時間初期値）から第1設定値（初期値よりも小さい値）までの期間における鍵管理に関する動作について説明する。

【0050】

この期間においては、コンテンツサーバ 1 1 内の鍵情報管理テーブル 2 1 は、使用中の鍵（暗号鍵および復号鍵）に関する鍵情報（鍵と鍵番号と残り有効時間との組）と、次に使用する鍵（暗号鍵および復号鍵）に関する鍵情報とを保持している。これらの鍵および鍵番号は、コンテンツサーバ 1 1 内の鍵管理手段 1 1 1 によって作成される。

【0051】

また、この期間においては、鍵管理サーバ 3 1 内の鍵情報管理テーブル 4 1 は、使用中の鍵（復号鍵）に関する鍵情報を保持している。

【0052】

さらに、この期間においては、各クライアント 5 i 内の鍵情報管理テーブル 6 i は、使用中の鍵（復号鍵）に関する鍵情報（コンテンツサーバ 1 1 から使用中の鍵によって暗号化されたデータを含むマルチキャストパケットを受信するまでは、次に使用する鍵の鍵情報として管理している）を保持している。また、コンテンツサーバ 1 1 から新たな使用中の鍵によって暗号化されたデータを有するマルチキャストパケットを受信するまでは、直前に使用中の鍵であった鍵に関する鍵情報も保持している。

10

【0053】

なお、この期間に新しくマルチキャストアドレスに参加したクライアント 5 i が存在する場合に、当該クライアント 5 i 内の鍵管理手段 5 i 1 が鍵管理サーバ 3 1 に鍵情報要求 8 1 を送信すると、鍵管理サーバ 3 1 内の鍵管理手段 3 1 1 は使用中の鍵に関する鍵情報を有する応答メッセージ 8 2 を当該クライアント 5 i に送信する。

【0054】

20

第 3 に、使用中の鍵の残り有効時間の値が第 1 設定値となった時点における鍵管理に関する動作について説明する（図 3 参照）。

【0055】

コンテンツサーバ 1 1 内の鍵管理手段 1 1 1 は、鍵情報管理テーブル 2 1 で管理している使用中の鍵の残り有効時間の値が第 1 設定値となったこと（残り有効時間の値が減っていった第 1 設定値に達したこと）を認識すると（ステップ B 1）、次に使用する鍵（復号鍵）に関する鍵情報（鍵番号と鍵と残り有効時間との組）を有するメッセージ（鍵情報メッセージ 7 1）を鍵管理サーバ 3 1 に対して送信する（ステップ B 2）。

【0056】

鍵管理サーバ 3 1 内の鍵管理手段 3 1 1 は、コンテンツサーバ 1 1 から鍵情報メッセージ 7 1 を受信すると（ステップ B 3）、その鍵情報メッセージ 7 1 中の次に使用する鍵に関する鍵情報を鍵情報管理テーブル 4 1 に保存する（ステップ B 4）。これによって、鍵管理サーバ 3 1 内の鍵情報管理テーブル 4 1 は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持することになる。

30

【0057】

なお、この時点から使用中の鍵の残り有効時間の値が後述の第 2 設定値となる時点までの期間において、新しくマルチキャストアドレスに参加したクライアント 5 i が存在する場合に、当該クライアント 5 i 内の鍵管理手段 5 i 1 が鍵管理サーバ 3 1 に鍵情報要求 8 1 を送信すると、鍵管理サーバ 3 1 内の鍵管理手段 3 1 1 は使用中の鍵に関する鍵情報と次に使用する鍵に関する鍵情報とを有する応答メッセージ 8 2 を当該クライアント 5 i に送信する。

40

【0058】

第 4 に、使用中の鍵の残り有効時間の値が第 2 設定値（第 1 設定値よりも小さい値であり 0 よりも大きい値）となった時点における鍵管理に関する動作について説明する（図 4 参照）。

【0059】

クライアント 5 i 内の鍵管理手段 5 i 1 は、自身の鍵情報管理テーブル 6 i 内の使用中の鍵の残り有効時間の値が第 2 設定値となった時に、そのこと（残り有効時間の値が減っていった第 2 設定値に達したこと）を認識し（ステップ C 1）、次に使用する鍵（復号鍵）に関する鍵情報を得るために、鍵管理サーバ 3 1 に対して鍵情報要求 8 1 を送信する（ス

50

テップC2)。なお、クライアント5iには、鍵情報要求81の送信先である鍵管理サーバ31のアドレスが、あらかじめ設定されている。

【0060】

鍵管理サーバ31内の鍵管理手段311は、クライアント5iからの鍵情報要求81を受信すると（ステップC3）、その応答として、現在使用中の鍵（復号鍵）に関する鍵情報と次に使用する鍵（復号鍵）に関する鍵情報とを有する応答メッセージ82を当該クライアント5iに送信する（ステップC4）。

【0061】

当該クライアント5iは、この応答メッセージ82を受信すると（ステップC5）、当該応答メッセージ82中の次に使用する鍵に関する鍵情報を自己の鍵情報管理テーブル6i

10

に保存する（ステップC6）。

【0062】

第5に、使用中の鍵の残り有効時間の値が0となった時点における鍵管理に関する動作について説明する。

【0063】

コンテンツサーバ11内の鍵管理手段111は、鍵情報管理テーブル21に保持されている使用中の鍵の残り有効時間が0となった時に、その使用中の鍵に関する鍵情報を破棄し、次に使用する鍵に関する鍵情報として保持されていた鍵情報を新たな使用中の鍵に関する鍵情報として鍵情報管理テーブル21に保存する。これにより、暗号化・パケット送信手段112は、その鍵を使用して以後の暗号化処理を行う。

20

【0064】

このときさらに、鍵管理手段111は、新たな次に使用する鍵（暗号鍵および復号鍵）を作成して、その次に使用する鍵に関する鍵情報を鍵情報管理テーブル21に保存する。

【0065】

また、暗号化・パケット送信手段112は、暗号化パケット（暗号化データを有するマルチキャストパケット）に含まれる鍵番号を新たな使用中の鍵に対する鍵番号に変更し、それにより、クライアント5iに対して使用中の鍵が変更されたことを示す。

【0066】

各クライアント5i内の鍵管理手段5i1は、コンテンツサーバ11から送られてきた暗号化パケット（パケット受信・復号化手段5i2により受信された暗号化パケット）に含まれる鍵番号が変更されたことを確認すると、自身の鍵情報管理テーブル6i内の当該鍵番号を持つ次に使用する鍵を新たな使用中の鍵として保存するようにする。このとき、当該各クライアント5iは、新たな次に使用する鍵をまだ得ていないため、自身の鍵情報管理テーブル6iにおいて次に使用する鍵に関する鍵情報を持たない状態となる。

30

【0067】

一方、鍵管理サーバ31内の鍵管理手段311は、鍵情報管理テーブル41に保持されている使用中の鍵に関する鍵情報中の残り有効時間が0となった時に、その使用中の鍵に関する鍵情報を破棄し、次に使用する鍵に関する鍵情報として保持されていた鍵情報を新たな使用中の鍵に関する鍵情報として鍵情報管理テーブル41に保存する。このとき、鍵管理サーバ31は、新たな次に使用する鍵をまだ得ていないため、鍵情報管理テーブル41

40

において次に使用する鍵に関する鍵情報を持たない状態となる。

【0068】

なお、残り有効時間の初期値、第1設定値（Xとする）および第2設定値（Yとする）の設定方法は、例えば、次のaまたはbに示すような方法が考えられる。

【0069】

a. 当該マルチキャスト配信システム全体で共通な設定値として、手動での設定を行う。

【0070】

b. 鍵の残り有効時間とともにその初期値を各装置（鍵管理サーバおよびクライアント）に送信することで、その初期値から一定の割合の時間をXおよびYとして各装置で求める。この「一定の割合」は、当該マルチキャスト配信システム全体で共通な設定とする。具

50

体例を挙げると、Xを鍵の残り有効時間の初期値の50%とし、Yを鍵の残り有効時間の初期値の25%とした場合に、鍵の残り有効時間の初期値が1時間であった際には、Xは30分となり、Yは15分となる。

【0071】

次に、図5および図6を参照して、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の具体的な動作（一連の動作シーケンス）について説明する。

【0072】

図5は、各鍵情報管理テーブル内の情報や、各パケット／要求／メッセージの内容を具体的に示す図である。なお、図5においては、使用中の鍵を鍵Aで示しており、次に使用する鍵を鍵Bで示しており、それらの鍵番号を「鍵番号A」および「鍵番号B」と表記している。また、この例では、暗号鍵と復号鍵とは同じ鍵であるものとする（例えば、鍵Aは暗号鍵でもあり、復号鍵でもある）。さらに、第1設定値をXで示しており、第2設定値をYで示している。

10

【0073】

図6は、図5に示すような内容の情報が取り扱われる場合の動作シーケンスを時間経過に沿って示した図である。

【0074】

この動作シーケンスでは、初期状態（鍵Aの残り有効時間の値が初期値である状態）において、コンテンツサーバ11は、使用中の鍵の鍵Aと次に使用する鍵の鍵Bとに関する鍵情報を持っている。また、鍵管理サーバ31およびクライアント51（ここでは、複数のクライアント51～5nの中からクライアント51に注目する）は、図5に示す鍵情報のうちの鍵Aに関する鍵情報のみを持っている。なお、残り有効時間の初期値や、XおよびYの値は、あらかじめ、コンテンツサーバ11、鍵管理サーバ31、およびクライアント51～5nに設定されているものとする。

20

【0075】

鍵Aの残り有効時間の値がX（第1設定値）となった時に、コンテンツサーバ11は、鍵B（次に使用する鍵）に関する鍵情報を有する鍵情報メッセージ71を鍵管理サーバ31に対して送信する。これにより、鍵管理サーバ31は、図5に示すように、鍵Aと鍵Bとに関する鍵情報を持つことになる。

【0076】

鍵Aの残り有効時間の値がY（第2設定値）となった時に、クライアント51は、鍵管理サーバ31に対して、次に使用する鍵に関する鍵情報を要求する鍵情報要求81を送信する。

30

【0077】

この鍵情報要求81を受けた鍵管理サーバ31は、応答として、現在使用中の鍵（鍵A）と次に使用する鍵（鍵B）とに関する鍵情報を有する応答メッセージ82を送信する。これにより、クライアント51は、図5に示すように、鍵Aと鍵Bとに関する鍵情報を持つことになる。

【0078】

鍵Aの残り有効時間の値が0となった時に、コンテンツサーバ11は、使用中の鍵である鍵Aに関する鍵情報を破棄し、保存していた次に使用する鍵である鍵Bを新たな使用中の鍵として保持し、その鍵Bを使用して配信データの暗号化を行う。また、この時に、コンテンツサーバ11は、新たな次に使用する鍵として鍵Cを生成し、この鍵Cに関する鍵情報を鍵情報管理テーブル21に保存する。この鍵Cに関する鍵情報は、鍵Bの残り有効時間がXとなった時に、鍵情報メッセージ71によって、コンテンツサーバ11から鍵管理サーバ31に対して送信される。

40

【0079】

鍵管理サーバ31は、鍵Aの残り有効時間の値が0となった時に、鍵Aに関する鍵情報を破棄し、次に使用する鍵として保存していた鍵Bを現在使用中の鍵として保持する。さらに、コンテンツサーバ11からの鍵情報メッセージ71によって鍵Cに関する鍵情報を受

50

け取ると、その鍵情報を次に使用する鍵に関する鍵情報として鍵情報管理テーブル 4 1 に保存する。これにより、鍵情報管理テーブル 4 1 に保持されている鍵情報は、図 5 中の鍵 A に関する鍵情報が鍵 B に関する鍵情報に入れ替わり、図 5 中の鍵 B に関する鍵情報が鍵 C に関する鍵情報に入れ替わった形となる。

【0080】

クライアント 5 1 は、コンテンツサーバ 1 1 から鍵 B の鍵番号を有するマルチキャストパケットを受信すると、鍵 A に関する鍵情報を破棄し、次に使用する鍵として保存していた鍵 B を現在使用中の鍵として保持する。さらに、鍵管理サーバ 3 1 からの応答メッセージ 8 2 によって鍵 B の次に使用する鍵である鍵 C に関する鍵情報を受け取ると、その鍵情報を自身の鍵情報管理テーブル 6 i に保存する。これにより、当該鍵情報管理テーブル 6 i に保持されている鍵情報は、図 5 中の鍵 A に関する鍵情報が鍵 B に関する鍵情報に入れ替わり、図 5 中の鍵 B に関する鍵情報が鍵 C に関する鍵情報に入れ替わった形となる。

10

【0081】

以上のような動作が繰り返されることによって、クライアント 5 1（一般的には、各クライアント 5 i）は鍵の変更が実行される前に、次に使用する鍵に関する鍵情報を取得することが可能になる。

【0082】

なお、本実施の形態においては、コンテンツサーバ 1 1、鍵管理サーバ 3 1、およびクライアント 5 i の間の通信に掛かる通信遅延は考慮されていない。したがって、そのような通信遅延の分だけ、各鍵情報管理テーブル 2 1、4 1、および 6 i における同一の鍵番号の鍵情報中の残り有効時間の値にずれが生じることも考えられる。このようなずれが実際に問題になる可能性は少ないが、これを考慮する際にも、以下の a および b に示すように、適切な対処が可能となる。

20

【0083】

a. 使用中の鍵の有効時間が切れる前（残り有効時間が 0 となる前）に次に使用する予定の鍵が使用された暗号化データ（その暗号化データと次に使用する鍵の鍵番号とを有するマルチキャストパケット）がきても、クライアント 5 i は、上記のような構成・動作によって、次に使用する鍵に関する鍵情報を保持しているため、鍵（復号鍵）の特定が可能であり、その復号鍵による解読（復号化）が可能となる。

【0084】

b. 有効時間が切れた後に古い鍵を使用した暗号化データが送られてきたとしても、クライアント 5 i は、残り有効時間が 0 となった後も、新たな使用中の鍵の鍵番号を有するマルチキャストパケットを受信するまでは、古い鍵に関する鍵情報を保持しているので、その鍵（復号鍵）による解読が可能となる。

30

【0085】

（2） 第 1 の実施の形態の変形形態

【0086】

上記のような第 1 の実施の形態に対しては、コンテンツサーバ 1 1 からクライアント 5 i に配信されるマルチキャストパケットに含まれる情報に関して、以下の a および b に示すような変形形態を考えることができる（a および b を併有する形態も可能である）。

40

【0087】

a. 上記の第 1 の実施の形態では、マルチキャストパケットは暗号化データと鍵番号とを有していたが、これに対して、さらに、鍵管理サーバ 3 1 のアドレス（アドレスと同様に問合せ先を示す情報を含む）を付加することも可能である。このように、マルチキャストパケット中に鍵管理サーバアドレスを付加して送ることによって、クライアント 5 i 側で鍵情報の問合せ・要求先（鍵情報要求 8 1 の送信先）の設定を不要にすることができる。

【0088】

b. また、マルチキャストパケットには、そのマルチキャストパケットが有している鍵番号で識別される鍵の残り有効時間を付加することも可能である。

【0089】

50

(3) 第2の実施の形態

【0090】

図7は、本発明の第2の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【0091】

図7を参照すると、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、マルチキャストパケットを送信するコンテンツサーバ12と、コンテンツサーバ12より送られたマルチキャストパケットを受信するクライアント51, 52, ..., 5n (nは正整数)と、コンテンツサーバ12から送られた鍵作成要求91に応じて鍵(暗号鍵および復号鍵)を作成・保管して当該暗号鍵とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組(鍵情報)を有する鍵情報応答メッセージ92をコンテンツサーバ12に返送し、クライアント5i (iは1~nの正整数)からの鍵情報要求81に対して応答メッセージ82を送信する鍵管理サーバ32と、コンテンツサーバ12, クライアント5i, および鍵管理サーバ32を接続するネットワーク100とを含んで構成されている。

10

【0092】

コンテンツサーバ12は、マルチキャストパケットによって配信されるデータの暗号化に用いる鍵(暗号鍵)とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組(鍵情報)を保持する鍵情報管理テーブル22を有する(鍵情報管理テーブルは鍵情報を複数保持しうる)。

20

【0093】

ここで、鍵情報管理テーブル22は、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。

【0094】

また、コンテンツサーバ12は、鍵管理手段121と、暗号化・パケット送信手段122とを含んで構成されている。

【0095】

鍵管理サーバ32は、鍵(暗号鍵・復号鍵)とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組(鍵情報)を保持する鍵情報管理テーブル42を有する。なお、本実施の形態では、鍵管理サーバ32によって鍵の作成が行われるので、鍵管理サーバ32の鍵情報管理テーブル42が暗号鍵と復号鍵とに関する鍵情報を保持している。

30

【0096】

ここで、鍵情報管理テーブル42は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持している。

【0097】

また、鍵管理サーバ32は、鍵管理手段321を含んで構成されている。

【0098】

クライアント5iは、マルチキャストパケットによって配信されるデータの復号化に用いる鍵(復号鍵)とその鍵を識別するための鍵番号とその鍵に対する残り有効時間との組(鍵情報)を保持する鍵情報管理テーブル6iを有する。

40

【0099】

ここで、鍵情報管理テーブル6iは、使用中の鍵に関する鍵情報を保持しており、次に使用する鍵に関する鍵情報を保持しうる。なお、初期状態では、鍵情報管理テーブル6iは情報を持っていない。

【0100】

また、クライアント5iは、鍵管理手段5i1と、パケット受信・復号化手段5i2とを含んで構成されている。

【0101】

なお、コンテンツサーバ12, 鍵管理サーバ32, および各クライアント5iは、それぞれの管理する鍵情報管理テーブル22, 鍵情報管理テーブル42, および各鍵情報管理テ

50

ーブル 6 i 上の鍵情報中の残り有効時間を時間の経過毎に更新する（自己のクロック信号に基づく更新等を行う）。

【0102】

本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、第 1 の実施の形態と比較して、コンテンツサーバ 1 2 が鍵管理サーバ 3 2 に対して鍵作成要求 9 1 を送信し、それに応じて、鍵管理サーバ 3 2 が鍵（暗号鍵・復号鍵）を作成し、作成した暗号鍵に関する鍵情報を有する鍵情報応答メッセージ 9 2 をコンテンツサーバ 1 2 に対して返送する点が異なっている。

【0103】

図 8 は、本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第 1 設定値となった時点における処理）を示す流れ図である。この処理は、第 1 設定値到達認識ステップ D 1 と、鍵作成要求送信ステップ D 2 と、鍵作成要求受信ステップ D 3 と、次使用鍵作成ステップ D 4 と、次使用鍵情報保存ステップ D 5 と、鍵情報応答メッセージ送信ステップ D 6 と、鍵情報応答メッセージ受信ステップ D 7 と、次使用鍵情報保存ステップ D 8 とからなる。

10

【0104】

次に、図 7 および図 8 を参照して（図 1 ～図 4 も適宜参照する）、上記のように構成された本実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の動作について、第 1 の実施の形態とは異なる点を中心に説明する。

【0105】

第 1 に、コンテンツサーバ 1 2 から各クライアント 5 i にネットワーク 1 0 0 を介して行われるマルチキャストパケット送受信処理に関する動作について説明する。

20

【0106】

この動作は、第 1 の実施の形態における動作（図 1 中のコンテンツサーバ 1 1 から各クライアント 5 i にネットワーク 1 0 0 を介して行われるマルチキャストパケット送受信処理に関する動作）と同様なものとなる。

【0107】

第 2 に、使用中の鍵の残り有効時間の値が初期値から第 1 設定値（初期値よりも小さい値）までの期間における鍵管理に関する動作について説明する。

【0108】

この期間においては、コンテンツサーバ 1 2 内の鍵情報管理テーブル 2 2 は、使用中の鍵（暗号鍵）に関する鍵情報（鍵と鍵番号と残り有効時間との組）を保持している。これらの鍵および鍵番号は、鍵管理サーバ 3 2 内の鍵管理手段 3 2 1 によって作成されたものである。

30

【0109】

また、この期間においては、鍵管理サーバ 3 2 内の鍵情報管理テーブル 4 2 は、使用中の鍵（暗号鍵・復号鍵）に関する鍵情報（鍵と鍵番号と残り有効時間との組）を保持している。これらの鍵および鍵番号は、鍵管理サーバ 3 2 内の鍵管理手段 3 2 1 によって作成されたものである。

【0110】

なお、上記以外の動作は、第 1 の実施の形態における動作と同様なものとなる。

40

【0111】

第 3 に、使用中の鍵の残り有効時間の値が第 1 設定値となった時点における鍵管理に関する動作について説明する（図 8 参照）。

【0112】

第 1 の実施の形態では、コンテンツサーバ 1 1 は、使用中の鍵の残り有効時間の値が第 1 設定値となったことを認識すると、鍵情報メッセージ 7 1 を鍵管理サーバ 3 1 に送信していた。

【0113】

これに対して、本実施の形態では、コンテンツサーバ 1 2 内の鍵管理手段 1 2 1 は、鍵情

50

報管理テーブル 2 2 で管理している使用中の鍵の残り有効時間の値が第 1 設定値となったこと（その時点に達したこと）を認識すると（ステップ D 1）、次に使用する鍵（暗号鍵）の鍵情報を得るために、鍵作成要求 9 1 を鍵管理サーバ 3 2 に対して送信する（ステップ D 2）。

【0114】

鍵管理サーバ 3 2 内の鍵管理手段 3 2 1 は、コンテンツサーバ 1 2 から鍵作成要求 9 1 を受信すると（ステップ D 3）、その鍵作成要求 9 1 に応じて、次に使用する鍵（暗号鍵・復号鍵）を作成し（ステップ D 4）、その鍵に関する鍵情報（鍵と鍵番号と残り有効時間との組）を鍵情報管理テーブル 4 2 に保存する（ステップ D 5）。これによって、鍵管理サーバ 3 2 内の鍵情報管理テーブル 4 2 は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持することになる。

10

【0115】

さらに、鍵管理手段 3 2 1 は、ステップ D 4 で作成した暗号鍵に関する鍵情報（暗号鍵と鍵番号と残り有効時間との組）を有する鍵情報応答メッセージ 9 2 をコンテンツサーバ 1 2 に送信（返送）する（ステップ D 6）。

【0116】

コンテンツサーバ 1 2 内の鍵管理手段 1 2 1 は、鍵管理サーバ 3 2 から鍵情報応答メッセージ 9 2 を受信すると（ステップ D 7）、その鍵情報応答メッセージ 9 2 中の次に使用する鍵（暗号鍵）に関する鍵情報を鍵情報管理テーブル 2 2 に保存する（ステップ D 8）。これによって、コンテンツサーバ 1 2 内の鍵情報管理テーブル 2 2 は、使用中の鍵に関する鍵情報と、次に使用する鍵に関する鍵情報とを保持することになる。

20

【0117】

なお、上記以外の動作は、第 1 の実施の形態における動作と同様なものとなる。

【0118】

第 4 に、使用中の鍵の残り有効時間の値が第 2 設定値（第 1 設定値よりも小さい値であり 0 よりも大きい値）となった時点における鍵管理に関する動作について説明する。

【0119】

この動作は、第 1 の実施の形態における動作と同様なものとなる。

【0120】

第 5 に、使用中の鍵の残り有効時間の値が 0 となった時点における鍵管理に関する動作について説明する。

30

【0121】

コンテンツサーバ 1 2 内の鍵管理手段 1 2 1 は、鍵情報管理テーブル 2 2 に保持されている使用中の鍵の残り有効時間が 0 となった時に、その使用中の鍵に関する鍵情報を破棄し、次に使用する鍵に関する鍵情報として保持されていた鍵情報を新たな使用中の鍵に関する鍵情報として鍵情報管理テーブル 2 2 に保存する。このとき、コンテンツサーバ 1 2 は、新たな次に使用する鍵をまだ得ていないため、鍵情報管理テーブル 2 2 において次に使用する鍵に関する鍵情報を持たない状態となる。

【0122】

これにより、暗号化・パケット送信手段 1 2 2 は、その鍵（暗号鍵）を使用して以後の暗号化処理を行う。

40

【0123】

なお、上記以外の動作は、第 1 の実施の形態における動作と同様なものとなる。

【0124】

前述の第 1 の実施の形態では、コンテンツサーバ 1 1 と鍵管理サーバ 3 1 との間の通信に障害が発生した際に、鍵（復号鍵）の配布ができなくなることがあった。これに対して、本実施の形態（第 2 の実施の形態）では、コンテンツサーバ 1 2 と鍵管理サーバ 3 2 との間の通信に障害が発生した際にも、以前の鍵を使い続けることで、暗号化データを有するマルチキャストパケットの通信を続けることが可能になる。

【0125】

50

このように、本発明では、上記の第1の実施の形態と第2の実施の形態とに示すように、鍵をコンテンツサーバで作成する構成も、鍵管理サーバで作成する構成も、実現することが可能である。

【0126】

(4) 第2の実施の形態の変形形態

【0127】

上記の第2の実施の形態に対しても、(2)のaおよびbで述べた第1の実施の形態に対する変形形態と同様の変形形態を考えることができる。

【0128】

(5) 第3の実施の形態

10

【0129】

図9は、本発明の第3の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【0130】

図9を参照すると、本発明の第3の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、図1に示した第1の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式に対して、コンテンツサーバ用鍵交換制御プログラム901、鍵管理サーバ用鍵交換制御プログラム902、およびクライアント用鍵交換制御プログラム903を備える点が異なっている。

【0131】

20

コンテンツサーバ用鍵交換制御プログラム901は、コンテンツサーバ11に読み込まれ、当該コンテンツサーバ11の動作を鍵情報管理テーブル21、鍵管理手段111、および暗号化・パケット送信手段112として制御する。コンテンツサーバ用鍵交換制御プログラム901の制御によるコンテンツサーバ11の動作（鍵情報管理テーブル21、鍵管理手段111、および暗号化・パケット送信手段112に関する動作）は、第1の実施の形態におけるコンテンツサーバ11の動作と全く同様になるので、その詳しい説明を割愛する。

【0132】

また、鍵管理サーバ用鍵交換制御プログラム902は、鍵管理サーバ31に読み込まれ、当該鍵管理サーバ31の動作を鍵情報管理テーブル41および鍵管理手段311として制御する。鍵管理サーバ用鍵交換制御プログラム902の制御による鍵管理サーバ31の動作（鍵情報管理テーブル41および鍵管理手段311に関する動作）は、第1の実施の形態における鍵管理サーバ31の動作と全く同様になるので、その詳しい説明を割愛する。

30

【0133】

さらに、クライアント用鍵交換制御プログラム903は、各クライアント5iに読み込まれ、当該各クライアント5iの動作を鍵情報管理テーブル6i、鍵管理手段5i1、およびパケット受信・復号化手段5i2として制御する。クライアント用鍵交換制御プログラム903の制御による各クライアント5iの動作（鍵情報管理テーブル6i、鍵管理手段5i1、およびパケット受信・復号化手段5i2に関する動作）は、第1の実施の形態におけるクライアント5iの動作と全く同様になるので、その詳しい説明を割愛する。

40

【0134】

(6) 第4の実施の形態

【0135】

図10は、本発明の第4の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【0136】

図10を参照すると、本発明の第4の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式は、図7に示した第2の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式に対して、コンテンツサーバ用鍵交換制御プログラム1001、鍵管理サーバ用鍵交換制御プログラム1002、およびクライアント用鍵交換制御プログラム1

50

003を備える点が異なっている。

【0137】

コンテンツサーバ用鍵交換制御プログラム1001は、コンテンツサーバ12に読み込まれ、当該コンテンツサーバ12の動作を鍵情報管理テーブル22、鍵管理手段121、および暗号化・パケット送信手段122として制御する。コンテンツサーバ用鍵交換制御プログラム1001の制御によるコンテンツサーバ12の動作（鍵情報管理テーブル22、鍵管理手段121、および暗号化・パケット送信手段122に関する動作）は、第2の実施の形態におけるコンテンツサーバ12の動作と全く同様になるので、その詳しい説明を割愛する。

【0138】

また、鍵管理サーバ用鍵交換制御プログラム1002は、鍵管理サーバ32に読み込まれ、当該鍵管理サーバ32の動作を鍵情報管理テーブル42および鍵管理手段321として制御する。鍵管理サーバ用鍵交換制御プログラム1002の制御による鍵管理サーバ32の動作（鍵情報管理テーブル42および鍵管理手段321に関する動作）は、第2の実施の形態における鍵管理サーバ32の動作と全く同様になるので、その詳しい説明を割愛する。

【0139】

さらに、クライアント用鍵交換制御プログラム1003は、各クライアント5iに読み込まれ、当該各クライアント5iの動作を鍵情報管理テーブル6i、鍵管理手段5i1、およびパケット受信・復号化手段5i2として制御する。クライアント用鍵交換制御プログラム1003の制御による各クライアント5iの動作（鍵情報管理テーブル6i、鍵管理手段5i1、およびパケット受信・復号化手段5i2に関する動作）は、第2の実施の形態におけるクライアント5iの動作と全く同様になるので、その詳しい説明を割愛する。

【0140】

【発明の効果】

以上説明したように、本発明によると、以下に示すような効果が生じる。

【0141】

第1の効果は、鍵の変更時に新しい鍵の取得のための遅延が発生しないことにある。すなわち、鍵交換遅延のないマルチキャスト配信時の鍵の変更が可能になるということである。このような効果が生じる理由は、鍵自体とともに鍵番号および鍵の残り有効時間を有する鍵情報を管理し、クライアントが使用中の鍵の有効期間内に次に使用する鍵をあらかじめ取得することができるようにすることにより、鍵を交換した際に即時に新しい鍵を用いて復号化を行うことができるためである。

【0142】

第2の効果は、クライアントがどのマルチキャストアドレスに参加する際でも鍵を要求する鍵管理サーバのアドレスを当該クライアントに設定する必要がなくなることにある。このような効果が生じる理由は、コンテンツサーバが送信するマルチキャストパケットに鍵管理サーバのアドレスを含めることができるため、クライアントはその鍵管理サーバアドレスに対して鍵の要求を行うことができるからである。

【0143】

第3の効果は、視聴者（クライアント）の情報を正確にリアルタイムに取得できることにある。このような効果が生じる理由は、本発明を用いることで鍵変更時の遅延がなくなるため、通信遅延を増大させずに鍵の変更サイクルを短くすることができ、クライアントの情報を鍵管理サーバで集計するサイクル（クライアントが復号化のために所定時間毎に鍵管理サーバに対して行う鍵取得の要求の際に当該クライアントの情報を鍵管理サーバで集計するサイクル）も短くでき、より正確なクライアントの情報を取得することができるからである。

【0144】

第4の効果は、「暗号化によって視聴者（クライアント）を限定し、許可しない相手が情報を取得することを防ぐ」という暗号化方式による利点を、より確実に実現することがで

10

20

30

40

50

きることにある。このような効果が生じる理由は、上記のように本発明では鍵を一定時間毎に変更することを効率的に実現できるため、万一鍵が漏れたとしても、鍵の変更により不正者が連続して視聴することを防ぐことができるからである。また、復号化に必要な鍵を管理する鍵管理サーバに視聴を許可する相手または許可しない相手を設定することで、復号鍵を渡す相手を特定することができるからでもある。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【図２】図１に示すマルチキャスト配信システムにおける鍵交換方式のマルチキャストパケット送受信処理を示す流れ図である。

10

【図３】図１に示すマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第１設定値となった時点における処理）を示す流れ図である。

【図４】図１に示すマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第２設定値となった時点における処理）を示す流れ図である。

【図５】図１に示すマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのブロック図である。

【図６】図１に示すマルチキャスト配信システムにおける鍵交換方式の具体的な動作を説明するためのシーケンス図である。

20

【図７】本発明の第２の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【図８】図７に示すマルチキャスト配信システムにおける鍵交換方式の鍵管理に関する処理（使用中の鍵の残り有効時間の値が第１設定値となった時点における処理）を示す流れ図である。

【図９】本発明の第３の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

【図１０】本発明の第４の実施の形態に係るマルチキャスト配信システムにおける鍵交換方式の構成を示すブロック図である。

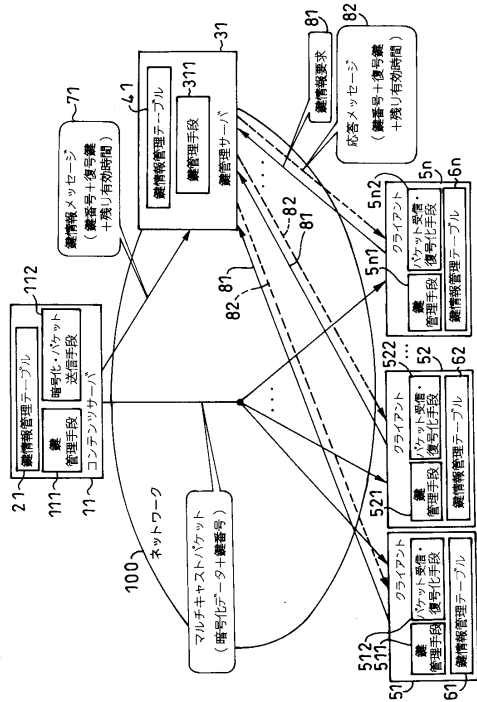
【符号の説明】

30

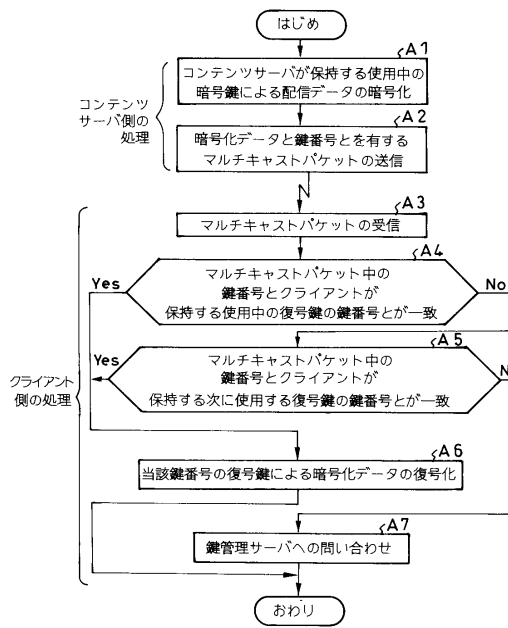
１１，１２ コンテンツサーバ
 ２１，２２，４１，４２，６１，６２，…，６ｎ 鍵情報管理テーブル
 ３１，３２ 鍵管理サーバ
 ５１，５２，…，５ｎ クライアント
 ７１ 鍵情報メッセージ
 ８１ 鍵情報要求
 ８２ 応答メッセージ
 ９１ 鍵作成要求
 ９２ 鍵情報応答メッセージ
 １００ ネットワーク
 １１１，１２１，３１１，３２１，５１１，５２１，…，５ｎ１ 鍵管理手段
 １１２，１２２ 暗号化・パケット送信手段
 ５１２，５２２，…，５ｎ２ パケット受信・復号化手段
 ９０１，１００１ コンテンツサーバ用鍵交換制御プログラム
 ９０２，１００２ 鍵管理サーバ用鍵交換制御プログラム
 ９０３，１００３ クライアント用鍵交換制御プログラム

40

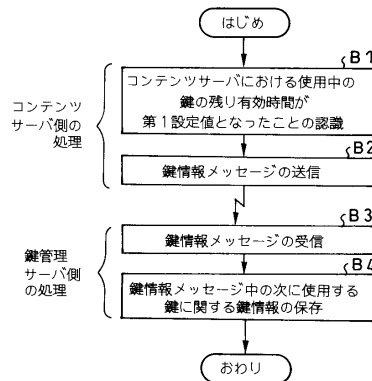
【図 1】



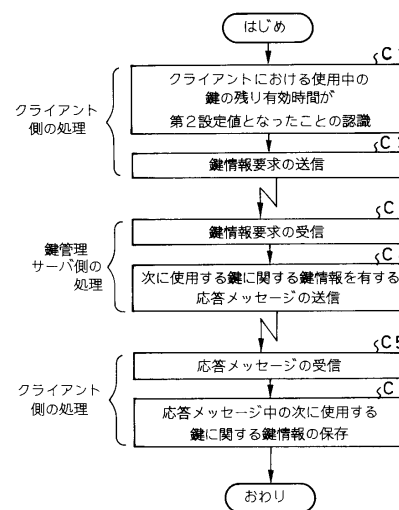
【図 2】



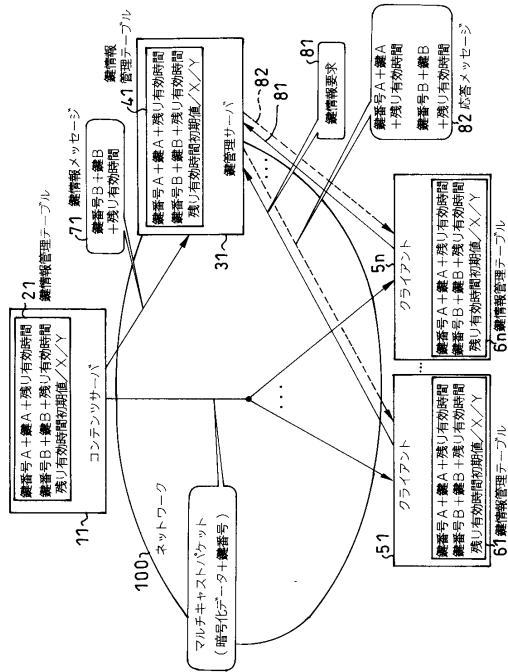
【図 3】



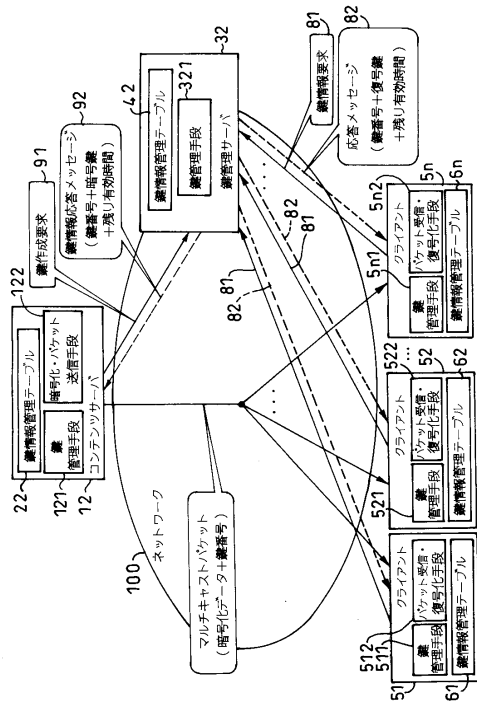
【図 4】



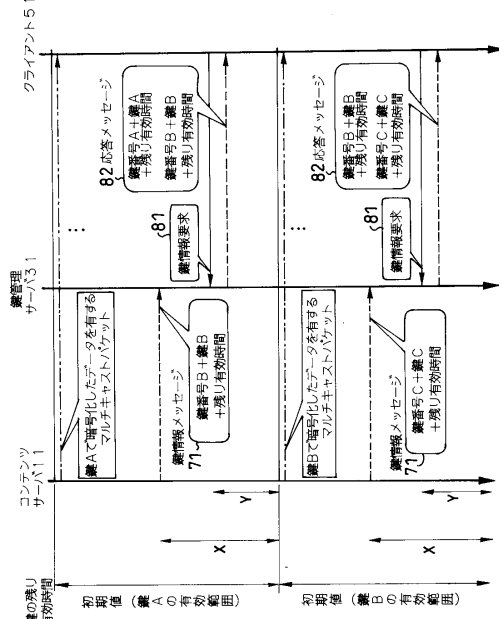
【図5】



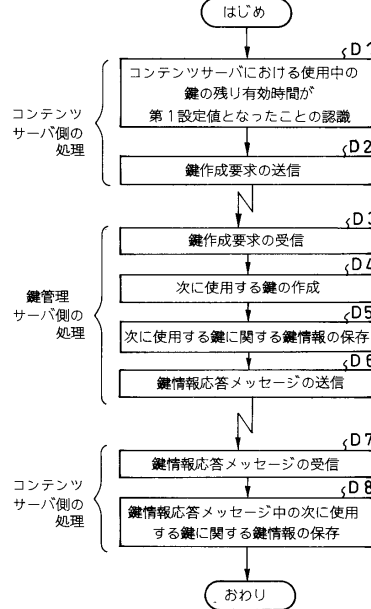
【図7】



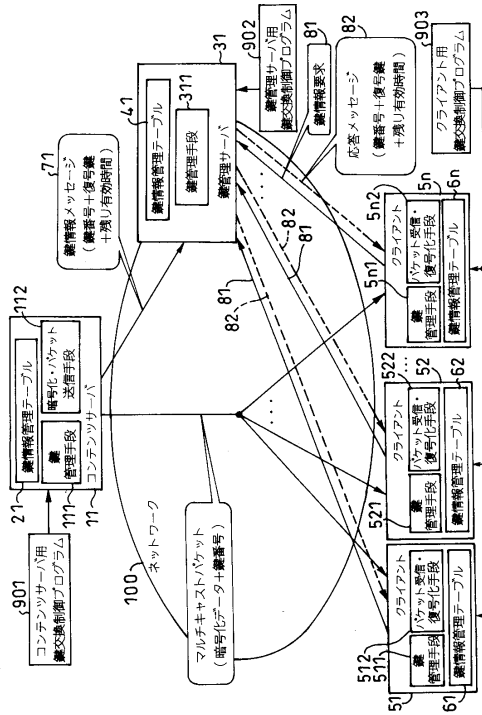
【図6】



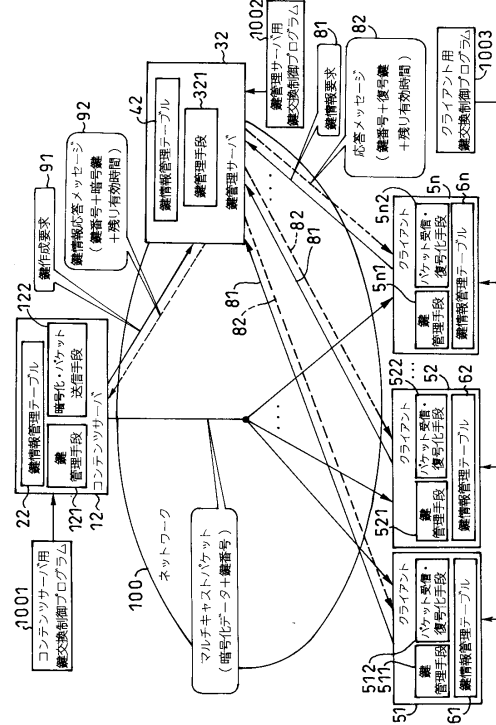
【図8】



【図 9】



【図 10】



フロントページの続き

(72)発明者 馬越 英之

東京都港区三田一丁目４番２８号 日本電気通信システム株式会社内

Fターム(参考) 5J104 AA16 AA34 BA03 EA01 EA04 EA18 JA03 MA05 NA02 PA05
PA07