(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-219912
(P2010-219912A)
(43)公開日　平成22年9月30日(2010.9.30)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601B	5J104
H04L	9/14	(2006.01)	H04L	9/00	601E	
			H04L	9/00	641	

審査請求 有　請求項の数 16　ＯＬ　（全 31 頁）

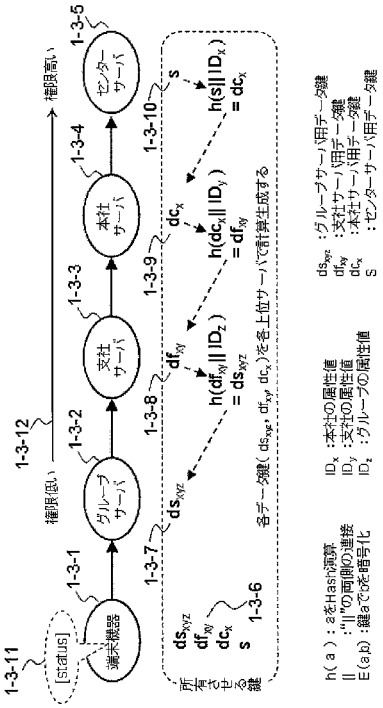
(21)出願番号　特願2009-64645 (P2009-64645)
(22)出願日　平成21年3月17日 (2009.3.17)

(71)出願人　000197366
ＮＥＣアクセステクニカ株式会社
静岡県掛川市下俣８００番地
(71)出願人　591107481
株式会社エルイーテック
東京都千代田区一ツ橋２丁目６番３号
(74)代理人　100077838
弁理士　池田　憲保
(74)代理人　100082924
弁理士　福田　修一
(74)代理人　100129023
弁理士　佐々木　敬
(72)発明者　浅田　英之
静岡県掛川市下俣８００番地　ＮＥＣアクセステクニカ株式会社内

最終頁に続く

(54)【発明の名称】暗号鍵生成方法、ネットワークシステム及びプログラム

(57)【要約】
【課題】
ネットワークシステムのサーバと端末機器との間で暗号通信するため、常に保持しておかなければならない暗号鍵の数を、サーバにて保持する暗号鍵、端末機器にて保持する暗号鍵の両方で削減する。
【解決手段】
第１のサーバの暗号鍵と第１のサーバの下位に接続された第２のサーバの属性値とを一方向性関数に入力して暗号鍵を生成する処理を第１のサーバにて実行し、生成した暗号鍵を第２のサーバの暗号鍵として第１のサーバから第２のサーバに送信する。これを階層化ネットワークシステムの上位サーバから下位サーバに向かって順次繰り返して各サーバの暗号鍵を生成する。
【選択図】　図３



【特許請求の範囲】
【請求項１】
サーバS_0、サーバS_0に接続されたサーバS_1、サーバS_1に接続されたサーバS_2、・・・、サーバS_{a-1}に接続されたサーバS_a（ａは予め定められた自然数）を備えるネットワークシステムの、サーバS_1、S_2、…、S_aの暗号鍵K_1、K_2、…、K_aを生成するため、
サーバS_{i-1}（ｉはａ以下の自然数）に対して予め定められた暗号鍵K_{i-1}と、サーバS_{i-1}に接続されたサーバS_iに対して予め定められた属性値ID_iとを、一方向性関数Ｆに入力して暗号鍵K_iを生成する処理を、サーバS_{i-1}が実行する段階１、及び、
暗号鍵K_iをサーバS_iに送信する処理をサーバS_{i-1}が実行する段階２を、
ｉ＝１、２、…、ａ－１の順に順次繰り返すことを特徴とする暗号鍵生成方法。
【請求項２】
請求項１に記載の暗号鍵生成方法において、
ネットワークシステムはサーバS_0を根ノードとし、サーバS_1、S_2、…、S_aをそれぞれ第１階層のノード、第２階層のノード、…、第ａ階層のノードとし、サーバS_aに接続された端末機器Ｔを葉ノードとする木構造を有し、
暗号鍵K_j（ｊはａ－１以下の自然数）の生成に先立って、属性値ID_jをサーバS_jに通知する処理をサーバS_0が実行する段階を含む
ことを特徴とする暗号鍵生成方法。
【請求項３】
請求項２に記載の暗号鍵生成方法において、サーバS_jの配下にあるサーバ及び端末機器に対し、サーバS_jの属性値ID_jを通知する処理をサーバS_0が実行する段階を含むことを特徴とする暗号鍵生成方法。
【請求項４】
請求項３に記載の暗号鍵生成方法において
端末機器Ｔと、サーバS_1、S_2、…、S_aのいずれかであるサーバS_x（ｘはａ以下の自然数）との間で暗号通信を行うための共通鍵方式の暗号鍵K_xを端末機器Ｔが取得するため、
予め取得したサーバS_0の暗号鍵K_0、及び、予め通知された属性値ID_1、ID_2、…、ID_xに基づいて、サーバS_{m-1}（ｍはａ以下の自然数）に対して予め定められた暗号鍵K_{m-1}と、サーバS_{m-1}に接続されたサーバS_mの属性値ID_mとを、一方向性関数Ｆに入力して暗号鍵K_mを生成する処理を、ｍがｘになるまでｍをひとつずつ増やしながら端末機器Ｔが繰り返し実行する
ことを特徴とする暗号鍵生成方法。
【請求項５】
請求項１乃至４のいずれかに記載の暗号鍵生成方法において、一方向性関数Ｆはハッシュ関数であることを特徴とする暗号鍵生成方法。
【請求項６】
サーバS_0、サーバS_0に接続されたサーバS_1、サーバS_1に接続されたサーバS_2、・・・、サーバS_{a-1}に接続されたサーバS_a（ａは予め定められた自然数）を備えるネットワークシステムであって、
サーバS_{i-1}（ｉ＝１、２、…、ａ）はそれぞれ、
サーバS_{i-1}に対して予め定められた暗号鍵K_{i-1}と、サーバS_{i-1}に接続されたサーバS_iに対して予め定められた属性値ID_iとを、一方向性関数Ｆに入力して暗号鍵K_iを生成する手段と、
生成した暗号鍵K_iをサーバS_iに送信する処理を実行する手段とを備える
ことを特徴とするネットワークシステム。
【請求項７】
請求項６に記載のネットワークシステムにおいて、

サーバS_0を根ノードとし、サーバS_1、S_2、…、S_aをそれぞれ第１階層のノード、第２階層のノード、…、第ａ階層のノードとし、サーバS_aに接続された端末機器Ｔを葉ノードとする木構造を有し、
サーバS_0は、暗号鍵K_j（ｊはａ－１以下の自然数）の生成に先立って、属性値ID_jをサーバS_jに通知する処理を実行する手段を備える
ことを特徴とするネットワークシステム。
【請求項８】
請求項７に記載のネットワークシステムにおいて、サーバS_0は、サーバS_jの配下にあるサーバ及び端末機器に対し、サーバS_jの属性値ID_jを通知する処理を実行する手段を備えることを特徴とするネットワークシステム。
【請求項９】
請求項８に記載のネットワークシステムにおいて、
端末機器Ｔと、サーバS_1、S_2、…、S_aのいずれかであるサーバS_x（ｘはａ以下の自然数）との間で暗号通信を行うための共通鍵方式の暗号鍵K_xを生成するため、
予め取得したサーバS_0の暗号鍵K_0、及び、予め通知された属性値ID_1、ID_2、…、ID_xに基づいて、サーバS_{m-1}（ｍはａ以下の自然数）に対して予め定められた暗号鍵K_{m-1}と、サーバS_{m-1}に接続されたサーバS_mの属性値ID_mとを、一方向性関数Ｆに入力して暗号鍵K_mを生成する処理を、ｍがｘになるまでｍをひとつずつ増やしながら繰り返し実行する手段を端末機器Ｔが備える
ことを特徴とするネットワークシステム。
【請求項１０】
請求項６乃至９のいずれかに記載のネットワークシステムにおいて、一方向性関数Ｆはハッシュ関数であることを特徴とするネットワークシステム。
【請求項１１】
請求項６乃至１０のいずれかに記載のネットワークシステムにおいて、
端末機器はそれぞれ自端末機器に固有の識別子である固有ＩＤを記憶する記憶装置を備え、
サーバS_b（ｂは０以上ａ以下の整数）は端末機器それぞれの固有ＩＤを記憶する記憶装置を備え、
サーバS_b及び端末機器は暗号鍵K_bを記憶する記憶装置を備え、
サーバS_bと一の端末機器は、それぞれ、その端末機器の固有ＩＤと暗号鍵K_bとを元に生成した暗号鍵を用いて、サーバS_bとその端末機器との間の暗号通信を行うことを特徴とするネットワークシステム。
【請求項１２】
サーバS_0、サーバS_0に接続されたサーバS_1、サーバS_1に接続されたサーバS_2、・・・、サーバS_{a-1}に接続されたサーバS_a（ａは予め定められた自然数）を備えるネットワークシステムのサーバS_0、S_1、S_2、…、S_{a-1}のいずれかのサーバの処理装置にて実行されて、
当該処理装置がサーバS_{i-1}（ｉはａ以下の自然数）の処理装置であるとき、
サーバS_{i-1}に対して予め定められた暗号鍵K_{i-1}と、サーバS_{i-1}に接続されたサーバS_iに対して予め定められた属性値ID_iとを、一方向性関数Ｆに入力して暗号鍵K_iを生成する手段、及び、
生成した暗号鍵K_iをサーバS_iに送信する処理を実行する手段
として当該処理装置を機能させるためのプログラム。
【請求項１３】
請求項１２に記載のプログラムにおいて、
ネットワークシステムは、サーバS_0を根ノードとし、サーバS_1、S_2、…、S_aをそれぞれ第１階層のノード、第２階層のノード、…、第ａ階層のノードとし、サーバS_aに接続された端末機器Ｔを葉ノードとする木構造を有し、
サーバS_0の処理装置にて実行され、

暗号鍵K_j（ｊはａ－１以下の自然数）の生成に先立って、属性値ID_jをサーバS_jに通知する処理を実行する手段としてサーバS_0の処理装置を機能させるためのプログラム。

【請求項１４】

請求項１３に記載のプログラムにおいて、サーバS_jの配下にあるサーバ及び端末機器に対してサーバS_jの属性値ID_jを通知する処理を実行する手段として、サーバS_0の処理装置を機能させるためのプログラム。

【請求項１５】

サーバS_0を根ノードとし、サーバS_1、S_2、…、S_aをそれぞれ第１階層のノード、第２階層のノード、…、第ａ階層のノードとし、サーバS_aに接続された端末機器Ｔを葉ノードとする木構造を有するネットワークシステムの端末機器Ｔの処理装置にて実行され、

端末機器Ｔと、サーバS_1、S_2、…、S_aのいずれかであるサーバS_x（ｘはａ以下の自然数）との間で暗号通信を行うための共通鍵方式の暗号鍵K_xを生成するため、

予め取得したサーバS_0の暗号鍵K_0、及び、予め通知された属性値ID_1、ID_2、…、ID_xに基づいて、サーバS_{m-1}（ｍはａ以下の自然数）に対して予め定められた暗号鍵K_{m-1}と、サーバS_{m-1}に接続されたサーバS_mの属性値ID_mとを、一方向性関数Ｆに入力して暗号鍵K_mを生成する処理を、ｍがｘになるまでｍをひとつずつ増やしながら繰り返し実行する手段として、端末機器Ｔの処理装置を機能させるプログラム。

【請求項１６】

請求項１２乃至１５のいずれかに記載のプログラムにおいて、一方向性関数Ｆはハッシュ関数であることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワークシステムにおいてサーバと端末機器の間で行う暗号通信に関し、特に、この種の暗号通信に使用する暗号鍵の生成及び管理に関する。

【背景技術】

【０００２】

ネットワークシステムにおいてサーバから複数の端末機器に対して制御コマンドやデータを送信することがある。第三者に内容を知られても構わないデータを送信するのであれば、送信先の複数の端末機器に対してそのデータを平文のままマルチキャストしても問題はないが、守秘性を有するデータであれば暗号化して送信するのが一般的であり、暗号化には暗号鍵の生成及び管理が不可欠である。

【０００３】

暗号化方式が共通鍵方式の場合、送信側と受信側に同じ暗号鍵を用意する必要がある。単純な方式では、暗号鍵を管理するサーバを用意し、このサーバにて各端末機器の暗号鍵を生成して保持する一方、それぞれの暗号鍵を該当する端末機器になんらかの経路で通知し、サーバと端末機器間で暗号通信を行う際には、この暗号鍵を用いて暗号化／復号化を行うことが考えられる。

【０００４】

このような方式では、暗号通信に先立って、サーバは全端末機器の暗号鍵を生成しておく必要がある。つまり、暗号鍵の生成処理の負荷は全てサーバに集中することになる。また、サーバは生成した暗号鍵を全て保持しておく必要があり、このためには端末機器の数に比例した記憶容量がサーバ乃至ネットワークシステムのどこかに必要となる。

【０００５】

更に、ネットワークシステムにはサーバを階層化するものがある。例えば、会社組織として、複数の本社があり、各本社の配下に複数の支社があり、更に各支社の配下に複数のグループがあるような組織構造を有するものを考える。このような会社組織にネットワークシステムを構築する際、センターサーバを中核として、その下層に本社毎に本社サーバ

を設置し、本社サーバの下層に支社毎に支社サーバを設置し、支社サーバの下層にグループ毎にグループサーバを設置し、各グループサーバの配下に端末機器を設置するといったネットワーク構成をとることがある。このようなネットワーク構成では、センターサーバは根ノードであり、端末機器は葉ノードとなる。センターサーバは本社サーバの親ノードであり、本社サーバは支社サーバの親ノードであり、支社サーバはグループサーバの親ノードである。

【０００６】

この種の階層化したネットワークシステムにおいて、上述のような暗号鍵と暗号通信を行うための暗号鍵を、センターサーバ、本社サーバ、支社サーバ、グループサーバのサーバの個々について用意すると、ネットワークシステム全体として生成・保持する暗号鍵の数は大きく膨れ上がる。どの階層のサーバも下流に接続された端末機器それぞれのための暗号鍵を生成して保持しなければならない。また、端末機器に対してその端末機器が属するセンターサーバ、本社サーバ、支社サーバ、グループサーバの４つの暗号鍵を通知する必要があり、端末機器ではこれら４つの暗号鍵を保持する必要がある。

【０００７】

また、この種の階層化したネットワークシステムでは、上層のサーバは下層のサーバよりも強い権限、即ち、下層のサーバのもつ権限を包括した権限を与えられることが多い。こういった権限の構造を、暗号通信を復号する権限として階層化ネットワークシステムに持ち込むには、上流のサーバは、自身の下流のサーバと更に下流の端末機器との間の暗号通信の復号が可能であるが、逆に、下流のサーバが上流のサーバと端末機器との間の暗号通信を復号することはできないようにサーバ、端末機器に暗号鍵を付与することが望ましい。上述したような単純な方式をベースとしてこのような階層的な復号の権限を実装しようとすると、下流のサーバと端末機器との間の暗号通信のための暗号鍵を、上流のサーバでも保持する必要がある。つまりグループサーバ‐端末機器間の暗号通信用の暗号鍵を、そのグループサーバの上流にある支社サーバ、本社サーバ、センターサーバが保持する必要があり、支社サーバ‐端末機器間用の暗号鍵をその支社サーバの上流の本社サーバ、センターサーバが保持する必要があり、本社サーバ‐端末機器間用の暗号鍵をセンターサーバが保持する必要がある。結果として、サーバが上層にあるほど保持すべき暗号鍵の数は増加し、ネットワークシステム全体として保持すべき暗号鍵は更に膨れ上がることになる。

【０００８】

本発明と関連する技術が記載された文献として特許文献１、特許文献２を挙げる。これらの文献には、サーバと端末機器との間で暗号通信を行うための暗号鍵の生成に関する従来の技術が記載されている。これら文献に記載のシステムではノードを複数のグループに分類しているがグループ間に上下関係はなく、端末機器から見てサーバは全て同一階層に属する。

【先行技術文献】

【特許文献】

【０００９】

【特許文献１】特開２００８－１２４８８４号公報

【特許文献２】特開２００８－１３１０７６号公報

【発明の概要】

【発明が解決しようとする課題】

【００１０】

本発明はこのような状況に鑑みてなされたものであり、本発明が解決しようとする課題は、ネットワークシステムのサーバと端末機器との間で暗号通信するため、常に保持しておかなければならない暗号鍵の数を、サーバが保持すべき暗号鍵の数についても端末機器が保持すべき暗号鍵の数についても削減し、ネットワークシステム全体としても削減することができる技術を提供することである。

【課題を解決するための手段】

【００１１】
上述の課題を解決するため、本発明は、次のような暗号鍵生成方法、ネットワークシステム及びプログラムを提供する。
【００１２】
まず、本発明の一態様として、サーバS_0、サーバS_0に接続されたサーバS_1、サーバS_1に接続されたサーバS_2、・・・、サーバS_{a-1}に接続されたサーバS_a（ａは予め定められた自然数）を備えるネットワークシステムの、サーバS_1、S_2、…、S_aの暗号鍵K_1、K_2、…、K_aを生成するため、サーバS_{i-1}（ｉはａ以下の自然数）に対して予め定められた暗号鍵K_{i-1}と、サーバS_{i-1}に接続されたサーバS_iに対して予め定められた属性値ID_iとを、一方向性関数Ｆに入力して暗号鍵K_iを生成する処理を、サーバS_{i-1}が実行する段階１、及び、暗号鍵K_iをサーバS_iに送信する処理をサーバS_{i-1}が実行する段階２を、ｉ＝１、２、…、ａ－１の順に順次繰り返すことを特徴とする暗号鍵生成方法を提供する。
【００１３】
また、本発明の他の一態様として、サーバS_0、サーバS_0に接続されたサーバS_1、サーバS_1に接続されたサーバS_2、・・・、サーバS_{a-1}に接続されたサーバS_a（ａは予め定められた自然数）を備えるネットワークシステムであって、サーバS_{i-1}（ｉ＝１、２、…、ａ）はそれぞれ、サーバS_{i-1}に対して予め定められた暗号鍵K_{i-1}と、サーバS_{i-1}に接続されたサーバS_iに対して予め定められた属性値ID_iとを、一方向性関数Ｆに入力して暗号鍵K_iを生成する手段と、生成した暗号鍵K_iをサーバS_iに送信する処理を実行する手段とを備えることを特徴とするネットワークシステムを提供する。
【００１４】
更に、本発明の他の一態様として、サーバS_0、サーバS_0に接続されたサーバS_1、サーバS_1に接続されたサーバS_2、・・・、サーバS_{a-1}に接続されたサーバS_a（ａは予め定められた自然数）を備えるネットワークシステムのサーバS_0、S_1、S_2、…、S_{a-1}のいずれかのサーバの処理装置にて実行されて、当該処理装置がサーバS_{i-1}（ｉはａ以下の自然数）の処理装置であるとき、サーバS_{i-1}に対して予め定められた暗号鍵K_{i-1}と、サーバS_{i-1}に接続されたサーバS_iに対して予め定められた属性値ID_iとを、一方向性関数Ｆに入力して暗号鍵K_iを生成する手段、及び、生成した暗号鍵K_iをサーバS_iに送信する処理を実行する手段として当該処理装置を機能させるためのプログラムを提供する。
【発明の効果】
【００１５】
本発明によれば、上位のサーバは、自身の暗号鍵と、自身よりも下位のサーバの属性値と、一方向性関数を元に自身よりも下位の全てのサーバの暗号鍵を算出することができるが、逆に下位のサーバでは、逆関数の計算が不可能乃至困難であるという一方向性関数の性質により、自身よりも上位のサーバの暗号鍵を算出することが困難乃至事実上できない。
【００１６】
このため、本発明によれば、上位のサーバには下位のサーバ宛の暗号通信の復号が可能であるが、逆に下位のサーバには上位のサーバ宛の暗号通信の復号が不可能であるといった状況を立ち上げることができる。いうなれば階層的な体系を有する暗号鍵の一群を生成することができる。ある階層よりも上位に属する一群のサーバでのみ復号可能な暗号を生成することができることとなるので、マルチキャストで送信しても指定した階層よりも上位のサーバのみで復号可能な暗号を生成することができる。一般に、この種の階層化したネットワークシステムでは、上位階層のサーバは下位階層のサーバよりも強いアクセス権を与えられる場合が多いが、本発明はこうしたアクセス権を付与するネットワークシステムに特に好適である。
【００１７】

各サーバの属性値と一方向性関数についてはネットワークシステム内で公開した状態で管理してもよい。下位サーバの暗号鍵については、下位サーバの暗号通信を復号する必要に応じて、自身の暗号鍵、下位サーバの属性値及び一方向性関数から算出可能なので、各サーバが保持するのは自身の暗号鍵のみでも構わない。最上位のサーバS_0はサーバS_1の属性値ID_1から暗号鍵K_1を求めてその直下の階層に属するサーバS_1に送信し、サーバS_1は暗号鍵K_1とその直下の階層に属するサーバS_2の属性値ID_2から暗号鍵K_2を求めてサーバS_2に送信するといったように、上位階層から下位階層に向かって逐次暗号鍵を求めることで、最終的にはサーバS_aの暗号鍵K_aまで求めることができる。同様にして、サーバS_1、S_2、…、S_aのどれでも自身より下位のサーバの暗号鍵を全て求めることができる。このため、各サーバが常時保持していければならない暗号鍵の数は自身の暗号鍵だけで済み、自身より下位のサーバの暗号鍵については必要に応じて生成することにしてもよい。このため、ネットワークシステム全体で常時保持すべき暗号鍵の数も少なくて済む。

【図面の簡単な説明】

【００１８】

【図１】本発明の一実施の形態であるネットワークシステム１００の木構造を説明するための図である。

【図２】ネットワークシステム１００のグループサーバ１－１－８～１－１－１５と端末機器１－２－１～１－２－３２の接続関係を説明するための図である。

【図３】センターサーバの秘密シードｓ、本社サーバのデータ鍵dc_x、支社サーバのデータ鍵df_{xy}、グループサーバのデータ鍵ds_{xyz}の生成関係と、サーバ間の権限の高低について説明するための図である。

【図４】センターサーバ、本社サーバ、支社サーバ、グループサーバそれぞれにおける、秘密シードｓ、データ鍵dc_x、df_{xy}、ds_{xyz}を用いての暗号通信の可否を示す表である。

【図５】本発明の実施例１において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図６】本発明の実施例１において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図７】本発明の実施例１において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図８】本発明の実施例１において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図９】本発明の実施例１において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図１０】本発明の実施例１において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図１１】グループサーバ２－１－８～２－１－１５と端末機器２－２－１～２－２－３２の接続関係を説明するための図である。

【図１２】秘密シードｓと本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zとを元に、センターサーバ、本社サーバ、支社サーバにてデータ鍵dc_x、df_{xy}、ds_{xyz}を順次生成していく過程を説明するための図である。

【図１３】本発明の実施例２において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図１４】本発明の実施例２において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図１５】本発明の実施例２において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図１６】本発明の実施例２において本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを各サーバに配信する方法について説明するための図である。

【図１７】本発明の実施例２において本社属性値ＩＤ$_x$、支社属性値ＩＤ$_y$、グループ属性値ＩＤ$_z$を各サーバに配信する方法について説明するための図である。
【図１８】本発明の実施例２において本社属性値ＩＤ$_x$、支社属性値ＩＤ$_y$、グループ属性値ＩＤ$_z$を各サーバに配信する方法について説明するための図である。
【図１９】本発明の実施例２において本社属性値ＩＤ$_x$、支社属性値ＩＤ$_y$、グループ属性値ＩＤ$_z$を各サーバに配信する方法について説明するための図である。
【図２０】本発明の実施例２において本社属性値ＩＤ$_x$、支社属性値ＩＤ$_y$、グループ属性値ＩＤ$_z$を各サーバに配信する方法について説明するための図である。
【図２１】グループサーバ３－１－８～３－１－１５と端末機器３－２－１～３－２－３２の接続関係を説明するための図である。
【図２２】秘密シードｓと本社属性値ＩＤ$_x$、支社属性値ＩＤ$_y$、グループ属性値ＩＤ$_z$とを元に、センターサーバ、本社サーバ、支社サーバにてデータ鍵ｄｃ$_x$、ｄｆ$_{xy}$、ｄｓ$_{xyz}$を順次生成していく過程を説明するための図である。
【発明を実施するための形態】
【００１９】
本発明の実施の形態であるネットワークシステム１００について説明する。図１に示すように、ネットワークシステム１００はセンターサーバ１－１－１を頂点とする木構造の階層構造を有するネットワークシステムである。センターサーバ１－１－１の階層の下には、上から順に本社サーバ階層、支社サーバ階層、グループサーバ階層がある。本社サーバ階層には本社サーバ１－１－２、１－１－３が属し、支社サーバ階層には支社サーバ１－１－４～１－１－７が属し、グループサーバ階層にはグループサーバ１－１－８～１－１－１５が属する。グループサーバには図２に示すように端末機器が接続されている。これらサーバ及び端末機器はコンピュータであり、いずれもコンピュータプログラムに従って動作する中央処理装置、主記憶装置、コンピュータプログラムやデータを格納する補助記憶装置、キーボード、マウス、ネットワークインタフェース装置、ディスプレイ等の入出力装置を備える。
【００２０】
ネットワークシステム１００の全サーバ及び全端末機器はそれぞれ鍵生成機能を備える。紙面の都合上、図１、２では、センターサーバ１－１－１、本社サーバ１－１－２、支社サーバ１－１－４、グループサーバ１－１－８、端末機器１－２－１のみがそれぞれ鍵生成機能１－１－１－１、１－１－２－１、１－１－３－１、１－１－８－１、１－２－１－１を備えるように記載しているが、実際には全てのサーバ、端末機器が鍵生成機能を備える。鍵生成機能は、専用の回路としてハードウェア的に実現してもよいし、或いは、サーバ、端末機器の不図示の処理装置にて実行されるプログラムとしてソフトウェア的に実現してもよい。
【００２１】
各サーバには所属する階層に応じた属性が付与される。センターサーバには属性［センター］が付与され、各本社サーバには属性［本社］が付与され、各支社サーバには属性［支社］が付与され、各グループサーバには属性［グループ］が付与される。ネットワークシステム１００は、［センター］を先頭に［本社］、［支社］、［グループ］の属性順にピラミッド構造を成している。つまり、ネットワークシステム１００はセンターサーバ１－１－１を根ノードとし、本社サーバを第１階層のノード、支社サーバを第２階層のノード、グループサーバを第３階層のノードとし、グループサーバに接続された端末機器を葉ノードとする木構造を有する。
【００２２】
サーバに与えられた属性はそのサーバが有する管理権限の強弱を示す。ここで管理権限とは他のサーバや端末機器を管理する権限である。ピラミッド構造の上位にあるサーバはそのサーバより下の階層に属するサーバ、端末機器の管理権限を有するものとする。例えば、センターサーバ１－１－１はネットワークシステム１００内の他の全サーバ及び全端末機器の管理権限を有する。本社サーバ１－１－２は、ピラミッド構造において自分の下

にあるサーバ及び端末機器、即ち、支社サーバ１－１－４、１－１－５、グループサーバ１－１－８、１－１－９、１－１－１０、１－１－１１、端末機器１－２－１～１－２－１６の管理権限を有するが、本社サーバ１－１－３及びその配下のサーバ、端末機器の管理権限は有していない。支社サーバ、グループサーバについても同様であり、ピラミッド構造において自分の配下のサーバ、端末機器の管理権限を有する。尚、サーバＡがサーバＢの配下にあるとは、サーバＡがサーバＢよりも下の階層に属し、かつ、サーバＡがサーバＢに直接、或いは、サーバＢの配下にある他のサーバを介して間接に接続されていることをいうものとする。

【００２３】

ピラミッド構造の最上位であるセンターサーバ１－１－１を除くサーバ、端末機器にはそれぞれ属性値が付与される。完全な属性値は属性［本社］、［支社］、［グループ］に対応する３つの属性値の組、即ち、本社属性値$ＩＤ_x$、支社属性値$ＩＤ_y$、グループ属性値$ＩＤ_z$からなる。属性［本社］、［支社］、［グループ］はそれぞれピラミッド構造をなす階層のひとつに対応する。本社属性値$ＩＤ_x$、支社属性値$ＩＤ_y$、グループ属性値$ＩＤ_z$を総称して階層属性値と呼ぶものとする。完全な属性値はピラミッド構造をなす全ての階層の階層属性値の組である。本実施の形態では本社サーバ及び支社サーバには完全な属性値を付与しない。図１においてサーバを示すブロックの中にある３桁の数字は、そのサーバの属性に対応する属性値である。例えば、本社サーバ１－１－２には$ＩＤ_x$＝００１が付与される。支社サーバ１－１－４、１－１－６にはそれぞれ$ＩＤ_y$＝００１が付与される。グループサーバ１－１－８、１－１－１０、１－１－１２、１－１－１４にはそれぞれ$ＩＤ_z$＝００１が付与される。

【００２４】

以下、本社属性値$ＩＤ_x$、支社属性値$ＩＤ_y$、グループ属性値$ＩＤ_z$の組からなる完全な属性値（$ＩＤ_x$、$ＩＤ_y$、$ＩＤ_z$）を単に属性値と呼ぶものとする。あるグループサーバの配下にある端末機器群には、ネットワークシステム１００においてセンターサーバ１－１－１からその端末機器群に至るまでの間に通過する本社サーバ、支社サーバ、グループサーバの本社属性値$ＩＤ_x$、支社属性値$ＩＤ_y$、グループ属性値$ＩＤ_z$からなる属性値（$ＩＤ_x$、$ＩＤ_y$、$ＩＤ_z$）が付与されて、端末機器群全体が一括表現される。例えば、端末機器１－２－１～１－２－４には、属性値（００１、００１、００１）が付与される。属性値（００１、００１、００１）はピラミッド構造の上位階層でこれらの端末機器に接続される本社サーバは$ＩＤ_x$＝００１であり、支社サーバは$ＩＤ_y$＝００１であり、グループサーバは$ＩＤ_z$＝００１であることを示す。図１において、各グループサーバの下に記載してあるのが属性値である。また、図２において、一のグループサーバの配下にある端末機器群を点線の四角形で囲んでいるが、四角形の底辺に沿って記載しているのがその端末機器群の属性値である。

【００２５】

属性値とは別に端末機器はそれぞれ固有ＩＤを有する。固有ＩＤはその端末機器に固有の識別子であり、例えばベンダー名に製造番号を連接したもので唯一無二の値である。図２において各端末機器の直下に記載したＮと３桁の数字を連接したものが固有ＩＤである。図２では、端末機器１－２－１～１－２－３２の固有ＩＤは順にＮ００１～Ｎ０３２である。

【００２６】

次に、図３を参照してネットワークシステム１００におけるデータ鍵の生成について説明する。ここで生成するデータ鍵は、各サーバと端末機器との間で暗号化したデータ通信を行う際に用いる共通鍵暗号方式の暗号鍵である。図３では、図１に示したブランチ構造の各属性［センター］、［本社］、［支社］、［グループ］、及び、図２に示した一グループサーバ配下の端末機器群のうち、親子関係にあるノードを抽象化し、センターサーバ１－３－５、本社サーバ１－３－４、支社サーバ１－３－３、グループサーバ１－３－２、端末機器１－３－１と記す。このような親子関係は、図１では例えばグループサーバ１－１－８、支社サーバ１－１－４、本社サーバ１－１－２、センターサーバ１－１－１の

間に成り立つ。また、グループサーバ１－１－１４、支社サーバ１－１－７、本社サーバ１－１－３、センターサーバ１－１－１の間に成り立つ。

【００２７】

端末機器１－３－１が接続されたある機器のステータス情報１－３－１１をデータ鍵で暗号化し、ネットワークを介してグループサーバ１－３－２、支社サーバ１－３－３、本社サーバ１－３－４あるいはセンターサーバ１－３－５へ送信する。この暗号化されたステータス情報１－３－１１は、その重要度に応じて、どの属性サーバで受信あるいは復号して良いかが端末機器１－３－１で定められている。この定めに従い、各属性のサーバがそれぞれに持つ受信権限の範囲内でそれら暗号化されたステータス情報１－３－１１を受信できることになる。ここで言う受信権限とは、データ鍵で暗号化されたステータス情報１－３－１１を受け取ったあるサーバが、それを復号できるか否かを意味し、そのサーバの受信権限の高低により区別されることを示す。

【００２８】

あるいは、ある属性のサーバから端末機器１－３－１へデータ鍵で暗号化されたコマンドを送信し、そのコマンドを受信した端末機器１－３－１は、送信相手サーバの送信権限の範囲内でそれらコマンドを受付けるか否か決定できる。ここでは、それら送信権限と受信権限を総称してアクセス権限と称すこととする。ここで、図１－３の場合、アクセス権限１－３－１２は、センターサーバ１－３－５側が高く、グループサーバ１－３－２側が低い。このため、端末機器１－３－１から送信されるデータ鍵で暗号化されたステータス情報１－３－１１は、４段階の階層を持ったそれぞれのデータ鍵１－３－６のいずれかによって暗号化される必要がある。なお、あるサーバから送信されるコマンドの場合も同様である。

【００２９】

データ鍵１－３－６は［センター］［本社］［支社］［グループ］の４つの階層のそれぞれに対応する４つのデータ鍵ｓ、dc_x、df_{xy}、ds_{xyz}からなる。これら４つのデータ鍵は、ある階層のデータ鍵と、その下の階層の属性に対応する属性値とを連接してハッシュ演算したものを、その下の階層のデータ鍵とすることを各階層で順次繰り返すことにより求める。

【００３０】

図３を参照すると、センターサーバ１－３－５のデータ鍵１－３－１０はｓそのものである。本社サーバ１－３－４のデータ鍵dc_x１－３－９は、その本社サーバ１－３－４の属性ID_xをｓに連接し、それをハッシュ演算した結果である。支社サーバ１－３－３のデータ鍵df_{xy}１－３－８は、その支社サーバ１－３－３の属性ID_yをdc_xに連接し、ハッシュ演算した結果である。グループサーバ１－３－２のデータ鍵ds_{xyz}１－３－７は、そのグループサーバ１－３－２の属性ID_zをdf_{xy}に連接し、ハッシュ演算した結果である。

【００３１】

一方、端末機器１－３－１は、上述の各サーバのデータ鍵ｓ、dc_x、df_{xy}、ds_{xyz}のすべてをデータ鍵１－３－６として保持する。暗号通信を行う際、端末機器１－３－１は、送信しようとしているステータス情報［ｓｔａｔｕｓ］の重要度に応じて適切なデータ鍵を選択し、選択したデータ鍵を用いて暗号化した暗号化データを送信する。

【００３２】

ネットワークシステム１００では、各サーバと端末機器とがこのようなデータ鍵を保持した後で、端末機器とサーバとの間で暗号通信を行う。暗号化に用いるデータ鍵を選択することによって、センターサーバ１－３－５以下のどのサーバまでで復号可能な暗号通信とするかを選択することができる。図４の表１－３－１３を参照して説明すると、グループサーバ用データ鍵ds_{xyz}にて暗号化したステータス情報［ｓｔａｔｕｓ］であるＥ（ds_{xyz}、［ｓｔａｔｕｓ］）は、グループサーバ１－３－２、支社サーバ１－３－３、本社サーバ１－３－４、センターサーバ１－３－５で復号可能である。支社サーバ用データ鍵df_{xy}にて暗号化したステータス情報［ｓｔａｔｕｓ］であるＥ（df_{xy}、

［ｓｔａｔｕｓ］）は、グループサーバ１－３－２では復号することができないが、支社サーバ１－３－３、本社サーバ１－３－４、センターサーバ１－３－５で復号可能である。本社サーバ用データ鍵dc_xにて暗号化したステータス情報［ｓｔａｔｕｓ］であるＥ（dc_x、［ｓｔａｔｕｓ］）は、グループサーバ１－３－２、支社サーバ１－３－３では復号することができないが、本社サーバ１－３－４、センターサーバ１－３－５で復号可能である。センターサーバ用データ鍵、即ち秘密シードｓにて暗号化したステータス情報［ｓｔａｔｕｓ］であるＥ（ｓ、［ｓｔａｔｕｓ］）はセンターサーバ１－３－５でのみ復号可能である。

【００３３】

センターサーバ１－３－５は自身のデータ鍵である秘密シードｓと属性値ID_x、ID_y、ID_zから容易に他サーバのデータ鍵を求めることができるのに対して、ハッシュ演算がもつ逆演算の困難性により、本社サーバ、支社サーバ、グループサーバでは秘密シードｓを求めることが事実上できない。また、本社サーバは自身のデータ鍵dc_xと属性値ID_y、ID_zから支社サーバ、グループサーバのデータ鍵を求めることができるが逆はできない。同様に、支社サーバは自身のデータ鍵df_{xy}と属性値ID_zからグループサーバのデータ鍵を求めることができるが逆はできない。このようにして、ネットワークシステム１００では、自分より下の階層に属するサーバのデータ鍵を各サーバは生成することができる一方、自分よりも上の階層に属するサーバのデータ鍵を生成することはできないようになる。

【００３４】

ネットワークシステム１００によれば、端末機器にてひとつの暗号鍵で暗号化処理を行うだけで、指定した上位階層に属するサーバでのみ復号可能な暗号を生成することができる。従来のように送信先のサーバ毎に異なるデータ鍵を用いて暗号化処理を実行する必要がなく、端末機器での暗号化処理の負荷を軽減することができる。

【００３５】

また、ネットワークシステム１００によれば、暗号化したデータを送信する際に、送信先のサーバ毎にユニキャスト通信を行う代わりにネットワークシステム全体に対してブロードキャストを行っても、所望のサーバでのみ復号可能であるので、ネットワーク負荷の軽減に資することができる。

【００３６】

また、ネットワークシステム１００によれば、常に保持しておかなければならないデータ鍵の数を従来に比べて少なくすることができる。

【００３７】

まず、管理する全ての端末機器それぞれのデータ鍵をセンターサーバの記憶装置に秘密状態で保持する必要がなく、秘密鍵ｓ、本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zを用いてハッシュ演算することにより必要に応じて通信相手の端末機器のデータ鍵を生成することができる。これらのうち、各属性値はネットワークシステム内で公開し、秘密鍵ｓのみを秘密状態で管理してもよい。このため、特に、端末機器の数が膨大な場合、端末機器毎にデータ鍵を管理する従来のシステムと比較して、ネットワークシステム全体でのデータ鍵の管理コストを軽減することができる。

【００３８】

同様に、端末機器にて管理しなければならないデータ鍵の数についても、秘密鍵ｓを保持した上で、他のデータ鍵dc_x、df_{xy}、ds_{xyz}については必要に応じて端末機器にて生成することとしてもよい。このようにすれば、各端末機器が常時記憶装置に保持しておかなければならないデータ鍵は秘密シードｓだけで済む。特に、ネットワークシステム全体で見たときの端末機器のデータ鍵の管理コストを低減することができる。

【実施例１】

【００３９】

上述の実施の形態では、本社属性値ID_x、支社属性値ID_y、グループ属性値ID_zは予めネットワークシステム１００内の各サーバ、端末機器に通知されていることを前提

として説明した。本実施例では、ネットワークシステム１００において本社属性値ＩＤ$_x$、支社属性値ＩＤ$_y$、グループ属性値ＩＤ$_z$を配信する方法について説明する。尚、センターサーバは配下の全てのサーバ及び端末機器のアドレス、特にマルチキャストアドレスを予め取得しているものとする。

【００４０】

はじめに以下の説明中で参照する図面について説明する。図５～１０はネットワークシステム１００に相当するネットワークシステムにおいて、ＩＰマルチキャストを用いてＩＤ$_x$、ＩＤ$_y$、ＩＤ$_z$を配信する過程を示すものである。図１１にはこのネットワークシステムにおいてグループサーバ２－１－８～２－１－１５の配下にある端末機器２－２－１～２－２－３２を図示している。ネットワークシステム１００ではＩＤ$_x$、ＩＤ$_y$、ＩＤ$_z$はそれぞれ００１または００２の値を取る為、属性値は２×２×２＝８通りであり、一の属性値が一のグループサーバに設定され、グループサーバの下位にある各端末機器には上位のグループサーバと同じ属性値が設定される。つまり同じグループサーバ配下の端末機器には同じ属性値が設定される。また、端末機器はそれぞれ固有ＩＤを備える。例えば、属性値（００１，００１，００１）が設定される４つの端末機器２－２－１、２－２－２、２－２－３、２－２－４は順にＮ００１、Ｎ００２、Ｎ００３、Ｎ００４を有する。固有ＩＤは例えばベンダー名に製造番号を連接した唯一無二のものである。

【００４１】

＜１回目：（１）ＩＤ$_x$＝００１をＩＰマルチキャスト通知＞

図５を参照して説明すると、センターサーバ２－１－１から、ＩＰマルチキャストパケットを使い、属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）のうちのＩＤ$_x$が００１であることを、本社サーバ２－１－２、及び、本社サーバ２－１－２に連なる親子関係を有するノードに順次送信していく。具体的には、図５の略左半分に図示した本社サーバ２－１－２、支社サーバ２－１－４、２－１－５、グループサーバ２－１－８～２－１－１１と、図１１の上段に図示した端末機器２－２－１～２－２－１６に対し、ＩＤ$_x$＝００１をＩＰマルチキャストする。端末機器２－２－１～２－２－１６にはその端末機器の親ノードにあたるグループサーバと同じ属性値が設定される。

【００４２】

このＩＰマルチキャストを受信した本社サーバ、支社サーバ、グループサーバの各サーバ及び端末機器は自身の属性値の本社属性値ＩＤ$_x$を次のようにセットする。

【００４３】

属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００１，？？？，？？？）

“？”は属性値が未設定であることを示す。

【００４４】

＜２回目：（１）ＩＤ$_x$＝００２をＩＰマルチキャスト通知＞

今度は図中の略右半分のノードに本社属性値ＩＤ$_x$＝００２を通知する。センターサーバ２－１－１から、ＩＰマルチキャストパケットを使い、属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）のうちのＩＤ$_x$が００２であることを本社サーバ２－１－３、支社サーバ２－１－６、２－１－７、グループサーバ２－１－１２～２－１－１５、端末機器２－２－１７～２－２－３２に送信する。

【００４５】

このＩＰマルチキャストを受信した本社サーバ、支社サーバ、グループサーバの各サーバ及び端末機器は自身の属性値の本社属性値ＩＤ$_x$を次のようにセットする。

【００４６】

属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００２，？？？，？？？）

尚、グループサーバ配下の各端末機器にはそのグループサーバと同じ属性値が設定される。

【００４７】

＜３回目：（２）ＩＤ$_y$＝００１をＩＰマルチキャスト通知＞

次に、本社サーバ２－１－２及び２－１－３それぞれの配下の図中左側の枝に連なる支

社サーバ、グループサーバ、端末機器に対しＩＤ$_y$＝００１を通知する。図７及び図１１を参照すると、本社サーバ２－１－２側では、属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）のうちのＩＤ$_y$が００１であることを、本社サーバ２－１－２、支社サーバ２－１－４、グループサーバ２－１－８、２－１－９、端末機器２－２－１～２－２－８に対して、センターサーバ２－１－１からＩＰマルチキャストパケットを使って送信する。同様に、本社サーバ２－１－３側では、本社サーバ２－１－３、支社サーバ２－１－６、グループサーバ２－１－１２、２－１－１３、端末機器２－２－１７～２－２－２４へセンターサーバ２－１－１からＩＰマルチキャストパケットを使って送信する。尚、この過程で、各本社サーバは、配下の支社サーバの支社属性値ＩＤ$_y$＝００１を取得する。

【００４８】

このようにして、支社サーバ２－１－４、２－１－６、グループサーバ２－１－８、２－１－９、２－１－１２、２－１－１３、及びこれらの配下の端末機器２－２－１～２－２－８、２－２－１７～２－２－２４の属性値の支社属性値ＩＤ$_y$を次のように定める。

【００４９】

属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００＊，００１，？？？）

記号“＊”はサーバ、端末機器によって異なる値が既定されていることを示す。例えばこの段階における端末機器２－２－１の属性値は（００１，００１，？？？）であり、端末機器２－２－１０の属性値は（００２，００１，？？？）である。

【００５０】

＜４回目：（２）ＩＤ$_y$＝００２をＩＰマルチキャスト通知＞

今度は、本社サーバ２－１－２及び２－１－３それぞれの配下の図中右側の枝に連なる支社サーバ、グループサーバ、端末機器に対しＩＤ$_y$＝００２を通知する。図８に示すように、属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）のうちのＩＤ$_y$が００２であることを、本社サーバ２－１－２、支社サーバ２－１－５、グループサーバ２－１－１０、２－１－１１、端末機器２－２－９～２－２－１６に対し、センターサーバ２－１－１からＩＰマルチキャストパケットを使って送信する。同様に、同様に、本社サーバ２－１－３側では、本社サーバ２－１－３、支社サーバ２－１－７、グループサーバ２－１－１４、２－１－１５、端末機器２－２－２５～２－２－３２へセンターサーバ２－１－１からＩＰマルチキャストパケットを使って送信する。尚、この過程で、各本社サーバは、配下の支社サーバの支社属性値ＩＤ$_y$＝００２を取得する。

【００５１】

このようにして、支社サーバ２－１－５、２－１－７、グループサーバ２－１－１０、２－１－１１、２－１－１４、２－１－１５、及びこれらの配下の端末機器２－２－９～２－２－１６、２－２－２５～２－２－３２の属性値の支社属性値ＩＤ$_y$を次のように定める。

【００５２】

属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００＊，００２，？？？）

例えばこの段階における端末機器２－２－９の属性値は（００１，００２，？？？）であり、端末機器２－２－２５の属性値は（００２，００２，？？？）である。

【００５３】

＜５回目：（３）ＩＤ$_z$＝００１をＩＰマルチキャスト通知＞

次に、図９に示すように、各支社サーバ配下の図中左側のグループサーバ及びそのグループサーバ配下の端末機器に対して、ＩＤ$_z$＝００１を通知する。属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）のうちのＩＤ$_z$が００１であることを、本社サーバ２－１－２、２－１－３、支社サーバ２－１－４～２－１－７、グループサーバ２－１－８、２－１－１０、２－１－１２、２－１－１４、端末機器２－２－１～２－２－４、２－２－９～２－２－１２、２－２－１７～２－２－２０、２－２－２５～２－２－２８に対して、センターサーバ２－１－１からＩＰマルチキャストパケットを使って送信する。尚、この過程で、各本社サーバ、各支社サーバは、配下のグループサーバのグループ属性値ＩＤ$_z$＝００１を取得する。

【００５４】
これにより、グループサーバ２－１－８、２－１－１０、２－１－１２、２－１－１４、端末機器２－２－１～２－２－４、２－２－９～２－２－１２、２－２－１７～２－２－２０、２－２－２５～２－２－２８に対して、属性値のグループ属性値$ＩＤ_z$を次のように定める。
【００５５】
属性値（$ＩＤ_x$，$ＩＤ_y$，$ＩＤ_z$）＝（００＊，００＊，００１）
例えば、端末機器２－２－１の属性値は（００１，００１，００１）であり、端末機器２－２－９の属性値は（００１，００２，００１）であり、端末機器２－２－１７の属性値は（００２，００１，００１）であり、端末機器２－２－２５の属性値は（００２，００２，００１）である。
【００５６】
＜６回目：（３）$ＩＤ_z$＝００２をＩＰマルチキャスト通知＞
次に、図１０に示すように、各支社サーバ配下の図中右側のグループサーバ及びそのグループサーバ配下の端末機器に対して、$ＩＤ_z$＝００２を通知する。属性値（$ＩＤ_x$，$ＩＤ_y$，$ＩＤ_z$）のうちの$ＩＤ_z$が００２であることを、本社サーバ２－１－２、２－１－３、支社サーバ２－１－４～２－１－７、グループサーバ２－１－９、２－１－１１、２－１－１３、２－１－１５、端末機器２－２－５～２－２－８、２－２－１３～２－２－１６、２－２－２１～２－２－２４、２－２－２９～２－２－３２に対して、センターサーバ２－１－１からＩＰマルチキャストパケットを使って送信する。尚、この過程で、各本社サーバ、各支社サーバは、配下のグループサーバのグループ属性値$ＩＤ_z$＝００２を取得する。
【００５７】
これにより、グループサーバ２－１－９、２－１－１１、２－１－１３、２－１－１５、端末機器２－２－５～２－２－８、２－２－１３～２－２－１６、２－２－２１～２－２－２４、２－２－２９～２－２－３２に対して、属性値のグループ属性値$ＩＤ_z$を次のように定める。
【００５８】
属性値（$ＩＤ_x$，$ＩＤ_y$，$ＩＤ_z$）＝（００＊，００＊，００２）
例えば、端末機器２－２－５の属性値は（００１，００１，００２）であり、端末機器２－２－１３の属性値は（００１，００２，００２）であり、端末機器２－２－２１の属性値は（００２，００１，００２）であり、端末機器２－２－２９の属性値は（００２，００２，００２）である。
【００５９】
このようにして、ネットワークシステム１００内のグループサーバ及び端末機器のそれぞれに対し、属性値（$ＩＤ_x$，$ＩＤ_y$，$ＩＤ_z$）を設定する。尚、以上の手順では、本社サーバに対して支社属性値$ＩＤ_y$、グループ属性値$ＩＤ_z$を設定することについては考慮していない。また、支社サーバに対して、グループ属性値$ＩＤ_z$を設定することについても考慮していない。
【００６０】
次に、図１２を参照して、ネットワークシステム１００におけるデータ鍵の生成について説明する。図１２では各サーバ、端末機器の鍵生成機能のみを取り上げている。
【００６１】
＜センターサーバにおける鍵生成機能２－１－１－１の動作＞
例えばセンターサーバ２－１－１のキーボードからの入力やサーバに内蔵する乱数生成機等により、センターサーバ２－１－１には予め秘密シードｓが与えられている。鍵生成機能２－１－１－１は、秘密シードｓと本社サーバそれぞれの本社属性値$ＩＤ_x$とを連接した値をハッシュ演算することにより、本社サーバ２－１－２のデータ鍵$ｄｃ_1$、本社サーバ２－１－３のデータ鍵$ｄｃ_2$を算出してセンターサーバ２－１－１に渡す。
【００６２】

$dc_1 = h(s||ID_{X1})$
$dc_2 = h(s||ID_{X2})$

【００６３】

センターサーバ２－１－１は、データ鍵dc_1、dc_2をそれぞれ配下の本社サーバ２－１－２、２－１－３へ送信する。

【００６４】

＜本社サーバにおける鍵生成機能２－１－２－１、２－１－３－１の動作＞

各本社サーバは、センターサーバから受け取った自身のデータ鍵と自身の配下の支社サーバの支社属性値ID_yとを連接した値をハッシュ演算することにより、その支社サーバのデータ鍵を生成する。

【００６５】

センターサーバ２－１－１から本社サーバ２－１－２がデータ鍵dc_1を受信すると、鍵生成機能２－１－２－１は、データ鍵dc_1と、配下の支社サーバ２－１－４の支社属性値ID_{y1}とを連接した値をハッシュ演算することにより、支社サーバ２－１－４のデータ鍵$df_{1.1}$を生成し、また、データ鍵dc_1と、配下の支社サーバ２－１－５の支社属性値ID_{y2}とを連接した値をハッシュ演算することにより、支社サーバ２－１－５のデータ鍵$df_{1.2}$を生成する。

【００６６】

同様にして、センターサーバ２－１－１から本社サーバ２－１－３がデータ鍵dc_2を受信すると、鍵生成機能２－１－３－１は、データ鍵dc_2と、配下の支社サーバ２－１－６の支社属性値ID_{y1}とを連接した値をハッシュ演算することにより、支社サーバ２－１－６のデータ鍵$df_{2.1}$を生成し、また、データ鍵dc_2と、配下の支社サーバ２－１－７の支社属性値ID_y2とを連接した値をハッシュ演算することにより、支社サーバ２－１－７のデータ鍵$df_{2.2}$を生成する。

【００６７】

$df_{1,1} = h(dc_1||ID_{y1})$
$df_{1,2} = h(dc_1||ID_{y2})$
$df_{2,1} = h(dc_2||ID_{y1})$
$df_{2,2} = h(dc_2||ID_{y2})$

【００６８】

鍵生成機能２－１－２－１からデータ鍵$df_{1.1}$、$df_{1.2}$を受け取った本社サーバ２－１－２は、それぞれのデータ鍵を対応する支社サーバ２－１－４、２－１－５に送信する。また、鍵生成機能２－１－３－１からデータ鍵$df_{2.1}$、$df_{2.2}$を受け取った本社サーバ２－１－３は、それぞれのデータ鍵を対応する支社サーバ２－１－６、２－１－７にも同様に送信する。

【００６９】

＜支社サーバにおける鍵生成機能２－１－４－１～２－１－７－１の動作＞

各支社サーバの鍵生成機能では、自身の上位の本社サーバから受け取った自身のデータ鍵と、自身の配下のグループサーバのグループ属性値ID_zとを連接した値をハッシュ演算することにより、そのグループサーバのデータ鍵を生成する。

【００７０】

支社サーバ２－１－４では、本社サーバ２－１－２からデータ鍵$df_{1,1}$を受信すると、鍵生成機能２－１－４－１は、このデータ鍵$df_{1,1}$と、支社サーバ２－１－４の配下のグループサーバ２－１－８のグループ属性値ID_{z1}とを連接した値をハッシュ演算することにより、グループサーバ２－１－８のデータ鍵$ds_{1,1,1}$を生成する。また、鍵生成機能２－１－４－１は、データ鍵$df_{1,1}$と、配下のもう一方のグループサーバ２－１－９のグループ属性値ID_{z2}とを連接した値をハッシュ演算することにより、グループサーバ２－１－９のデータ鍵$ds_{1,1,2}$を生成する。

【００７１】

つまり、支社サーバ２－１－４の鍵生成機能２－１－４－１では、次の演算を行うこと

により、グループサーバ２－１－８のデータ鍵$ds_{1,1,1}$、グループサーバ２－１－９のデータ鍵$ds_{1,1,2}$を生成する。

【００７２】

$ds_{1,1,1}=h(df_{1,1}||ID_{Z1})$

$ds_{1,1,2}=h(df_{1,1}||ID_{Z2})$

【００７３】

支社サーバ２－１－５の鍵生成機能２－１－５－１では、次の演算を行うことにより、グループサーバ２－１－１０のデータ鍵$ds_{1,2,1}$、グループサーバ２－１－１１のデータ鍵$ds_{1,2,2}$を生成する。

【００７４】

$ds_{1,2,1}=h(df_{1,2}||ID_{Z1})$

$ds_{1,2,2}=h(df_{1,2}||ID_{Z2})$

【００７５】

支社サーバ２－１－６の鍵生成機能２－１－６－１では、次の演算を行うことにより、グループサーバ２－１－１２のデータ鍵$ds_{2,1,1}$、グループサーバ２－１－１３のデータ鍵$ds_{2,1,2}$を生成する。

【００７６】

$ds_{2,1,1}=h(df_{2,1}||ID_{Z1})$

$ds_{2,1,2}=h(df_{2,1}||ID_{Z2})$

【００７７】

支社サーバ２－１－７の鍵生成機能２－１－７－１では、次の演算を行うことにより、グループサーバ２－１－１４のデータ鍵$ds_{2,2,1}$、グループサーバ２－１－１５のデータ鍵$ds_{2,2,2}$を生成する。

【００７８】

$ds_{2,2,1}=h(df_{2,2}||ID_{Z1})$

$ds_{2,2,2}=h(df_{2,2}||ID_{Z2})$

【００７９】

このようにしてグループサーバのデータ鍵を生成すると、各支社サーバは、配下のグループサーバに対し、そのグループサーバのデータ鍵を送信する。上記サーバー間でのデータ鍵の受け渡しは事前に用意されたデータ鍵受け渡し用の暗号鍵で暗号化して行われる。

【００８０】

＜端末機器における鍵生成機能２－２－１－１～２－２－３２－１の動作＞

図５～１０を参照して行った説明により、ネットワークシステム１００内の全ての端末機器に対して属性値を通知した。これらの属性値における本社属性値はその端末機器を配下とする本社サーバの本社属性値と同じである。同様に、端末機器の属性値の支社属性値は、その端末機器を配下とする支社サーバの支社属性値と同じであり、また、端末機器の属性値のグループ属性値は、その端末機器を配下とするグループサーバのグループ属性値と同じである。つまり、端末機器は、自身の属性値から、自身を配下とする本社サーバの本社属性値、支社サーバの支社属性値、グループサーバのグループ属性値を取得することができる。

【００８１】

一方で、端末機器２－２－１～２－２－３２には秘密シードｓを通知しておく。この通知は例えばセンターサーバ２－１－１から各端末機器にユニキャストやブロードキャストで送信することによって行う。公開鍵暗号方式を用いて通知する例として、センターの公開鍵を端末機器が取得可能な状態で、秘密シードｓをセンターの秘密鍵で暗号化し、各端末機器に暗号化した秘密シードｓを送信するものがある。或いは、予め端末機器の記憶装置に秘密シードｓを記憶しておくことで実現してもよい。

【００８２】

端末機器２－２－１～２－２－３２はそれぞれ鍵生成機能２－２－１－１～２－２－３２－１を備える。鍵生成機能２－２－１－１～２－２－３２－１はそれぞれ、その端末機

器の属性値（ID_x，ID_y，ID_z）と秘密シードｓとを元に、その端末機器を配下とする本社サーバ、支社サーバ、グループサーバのデータ鍵を生成する。

【００８３】

これらサーバのデータ鍵は、そのサーバの上位のサーバのデータ鍵と、そのサーバが属する階層に対応する属性値とを連接した値をハッシュ演算することにより求める。センターサーバのデータ鍵は秘密シードｓである。秘密シードｓと本社属性値ID_xとを連接した値をハッシュ演算して本社サーバのデータ鍵dc_xを生成し、生成したデータ鍵dc_xと支社属性値ID_yとを連接した値をハッシュ演算して支社サーバのデータ鍵df_{xy}を生成し、生成したデータ鍵df_{xy}とグループ属性値ID_zとを連接した値をハッシュ演算してグループサーバのデータ鍵ds_{xyz}を生成する。同一グループサーバ配下にある端末機器のデータ鍵dc_x、df_{xy}、ds_{xyz}は共通である。

【００８４】

例えば、グループサーバ２－１－８の配下である端末機器２－２－１～２－２－４においては、鍵生成機能２－２－１－１～２－２－４－１は、本社サーバ２－１－２のデータ鍵dc_1、支社サーバ２－１－４のデータ鍵$df_{1,1}$、グループサーバ２－１－８のデータ鍵$ds_{1,1,1}$を次の演算を実行して生成する。

【００８５】

$dc_1 = h(s||ID_{X1})$

$df_{1,1} = h(dc_1||ID_{y1})$

$ds_{1,1,1} = h(df_{1,1}||ID_{Z1})$

【００８６】

また、例えば、グループサーバ２－１－９の配下である端末機器２－２－５～２－２－８においては、鍵生成機能２－２－５－１～２－２－８－１は、本社サーバ２－１－２のデータ鍵dc_1、支社サーバ２－１－４のデータ鍵$df_{1,1}$、グループサーバ２－１－９のデータ鍵$ds_{1,1,2}$を次の演算を実行して生成する。

【００８７】

$dc_1 = h(s||ID_{X1})$

$df_{1,1} = h(dc_1||ID_{y1})$

$ds_{1,1,2} = h(df_{1,1}||ID_{Z2})$

【００８８】

別の例としては、グループサーバ２－１－１５の配下である端末機器２－２－２９～２－２－３２においては、鍵生成機能２－２－２９－１～２－２－３２－１は、本社サーバ２－１－３のデータ鍵dc_2、支社サーバ２－１－７のデータ鍵$df_{2,2}$、グループサーバ２－１－１５のデータ鍵$ds_{2,2,2}$を次の演算により生成する。

【００８９】

$dc_2 = h(s||ID_{X2})$

$df_{2,2} = h(dc_2||ID_{y2})$

$ds_{2,2,2} = h(df_{2,2}||ID_{Z2})$

【００９０】

＜暗号通信＞

図１２に示すように、センターサーバ２－１－１、本社サーバ２－１－２、２－１－３、支社サーバ２－１－４～２－１－７、グループサーバ２－１－８～２－１－１５は、それぞれ、自身のデータ鍵として秘密シードｓ、データ鍵ｄｃ、ｄｆ、ｄｓを取得する一方、端末機器２－２－１～２－２－３２は、それぞれ自身を配下とするセンターサーバ、本社サーバ、支社サーバ、グループサーバの秘密鍵ｓ、データ鍵ｄｃ、ｄｆ、ｄｓを取得した。

【００９１】

各端末機器は秘密シードｓを含む４種類のデータ鍵を適宜使い分けて暗号通信を行うことにより、図４に示すように、復号可能なサーバを階層化した暗号化情報を生成することができる。

【００９２】
以上、本実施例によれば、各階層におけるデータ鍵は、自己の階層より１つ上の階層の属性から順次計算して与えるので、データ鍵を生成するための演算処理を多数のサーバにて分散処理することができる。つまり、K_1を予め与えられた秘密シードｓとし、ｍを２以上の自然数、階層L_mのデータ鍵をK_m、階層L_mの階層属性値をA_m、階層L_mに属するサーバをS_mと表すとき、本実施の形態では、求めようとするデータ鍵K_mの階層L_mのひとつ上の階層L_{m-1}のデータ鍵K_{m-1}と、階層L_mの階層属性値A_mとを連接し、連接した値$K_{m-1}||A_m$をハッシュ演算して$K_m=h(K_{m-1}||A_m)$を求める処理を、階層L_{m-1}のサーバS_{m-1}において実行した後、求めたデータ鍵K_mをサーバS_{m-1}からサーバS_mに通知する。このような処理を上位の階層から下位の階層に向かって順次繰り返すことにより、ネットワークシステム内のすべてのサーバのデータ鍵を生成する。各サーバは自分の直下の階層に属するサーバの数だけハッシュ演算を行う。このため、一箇所のセンターサーバ等にてデータ鍵の生成処理を実行する従来の技術と比較すると、生成処理のための負荷を複数のコンピュータに分散して実行することができる点で異なる。
【００９３】
また、本実施例によれば、ネットワークシステム内のデータ鍵同士の間に、ネットワークシステムを構成するサーバ間の階層構造に似た階層構造を与えることができる。ネットワークシステム１００において、各サーバは、階層構造の上位にあるサーバから自身のデータ鍵を通知される一方、その配下の下位のサーバに対しそのサーバの階層属性値を通知する過程で、これら下位サーバの階層属性値を取得し、自身のデータ鍵と下位サーバの階層属性値から、直下の階層のサーバのデータ鍵だけではなく、更にその下の階層のサーバのデータ鍵をも必要に応じて生成することができる。逆に、下位階層のサーバは、自身のデータ鍵と上位階層のサーバの階層属性値とから上位階層サーバのデータ鍵を求めるのは極めて困難である。これはハッシュ演算の逆演算が困難であることによる。
【００９４】
また、本実施例によれば、端末機器に対して上位階層のサーバ全てのデータ鍵を通知する必要はなく、秘密シードｓとその端末機器の属性値（ID_x、ID_y、ID_z）を通知するだけでよい。各サーバと暗号通信する際に用いるデータ鍵は、上位サーバのデータ鍵から順にハッシュ演算にて求めることができるからである。
【実施例２】
【００９５】
実施例２のネットワークシステムのネットワーク構造は、実施例１のネットワークシステムと同じであるが、参照符号の先頭の数字が異なる。例えば、実施例１ではセンターサーバの参照符号は２－１－１であるが、実施例２のセンターサーバの参照符号は３－１－１である。本社サーバ、支社サーバ、グループサーバ、端末機器、鍵生成機能の参照符号についても同様である。
【００９６】
上述の実施例１では、端末機器及びグループサーバに完全な属性値を割り当てたが、本実施例では、端末機器及びグループサーバに加えて本社サーバ及び支社サーバにも完全な属性値を割り当てる点で異なる。
【００９７】
本来、本社サーバは支社の属性を有していないが、本社サーバの支社属性値ID_yを０００と定義する。同様に、本社サーバ及び支社サーバはグループの属性を有していないが、本社サーバ及び支社サーバのグループ属性値ID_zを０００と定義する。
【００９８】
本社サーバ、支社サーバ、グループサーバ、端末機器への完全な属性値の通知は、図１３から図２０に示す８回のＩＰマルチキャスト通信により行う。これら８回のＩＰマルチキャスト通信のうち、１回目（図１３）、２回目（図１４）、４回目（図１６）、５回目（図１７）、７回目（図１９）、８回目（図２０）は、それぞれ、実施例１において説明

した１～６回目（図５～１０）に順に対応する。例えば、本社属性値ＩＤ$_x$＝００１及びＩＤ$_x$＝００２のマルチキャスト通知動作は図１３及び図１４に示すようにして行われるが、この動作は、参照符号の先頭の数字が異なる点を除けば実施例１にて図５及び図６を参照して行った動作と同様である。このため、ここでは実施例１と同様の動作については説明を省略し、実施例１では行わなかった３回目（図１５）、６回目（図１８）の動作について説明する。

【００９９】

＜３回目：（２）ＩＤ$_y$＝０００をＩＰマルチキャスト通知＞

図１５に示すように、センターサーバ３－１－１からＩＰマルチキャストパケットを用いて、属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）のうちの支社属性値ＩＤ$_y$が０００であることを本社サーバ３－１－２、および本社サーバ３－１－３に通知する。この通知に応じて各本社サーバは自身の属性値を次のように設定する。

【０１００】

本社サーバ３－１－２：
（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００１，０００，？？？）
本社サーバ３－１－３：
（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００２，０００，？？？）

【０１０１】

＜６回目：（３）ＩＤ$_z$＝０００をＩＰマルチキャスト通知＞

図１８に示すように、センターサーバ３－１－１からＩＰマルチキャストパケットを使い、属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）のうちのグループ属性値ＩＤ$_z$が０００であることを、本社サーバ３－１－２、３－１－３、支社サーバ３－１－４、３－１－５、３－１－６、３－１－７へ送信する。これにより本社サーバ及び支社サーバの属性値は次のように設定される。

【０１０２】

本社サーバ３－１－２：
（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００１，０００，０００）
本社サーバ３－１－３：
（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００２，０００，０００）
支社サーバ３－１－４：
（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００１，００１，０００）
支社サーバ３－１－５：
（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００１，００２，０００）
支社サーバ３－１－６：
（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００２，００１，０００）
支社サーバ３－１－７：
（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）＝（００２，００２，０００）

【０１０３】

実施例１にて行ったＩＰマルチキャスト通信に加えて、図１５及び１８のＩＰマルチキャスト通信を行うことにより、本社サーバ、支社サーバ、グループサーバ、端末機器に対して、本社属性値ＩＤ$_x$、支社属性値ＩＤ$_y$、グループ属性値ＩＤ$_z$からなる完全な属性値（ＩＤ$_x$，ＩＤ$_y$，ＩＤ$_z$）を設定する。各端末機器３－２－１～３－２－３２には、図２１に示すように、それぞれその端末機器が接続されたグループサーバの属性値が設定される。本社サーバと支社サーバにて属性値の形式が同じために、属性値からデータ鍵を算出する鍵生成機能として、本社サーバと支社サーバはほとんど同じ条件の処理を適用することができる。

【０１０４】

次に、センターサーバ、本社サーバ、支社サーバ、端末機器の鍵生成機能にて行うデータ鍵の算出について図２２を参照して説明する。

【０１０５】

＜センターサーバの鍵生成機能３－１－１－１の動作＞
センターサーバ３－１－１の鍵生成機能３－１－１－１では、秘密シードのｓと本社サーバの属性値$ＩＤ_{x}$をハッシュ演算することにより、本社サーバのデータ鍵を算出する。
【０１０６】
本社サーバ３－１－２のデータ鍵$ｄｃ_{1,0,0}$：
$ｄｃ_{1,0,0}＝ｈ（ｓ||ＩＤ_{X1}）$
本社サーバ３－１－３のデータ鍵$ｄｃ_{2,0,0}$：
$ｄｃ_{2,0,0}＝ｈ（ｓ||ＩＤ_{X2}）$
【０１０７】
データ鍵生成後、センターサーバ３－１－１は、データ鍵$ｄｃ_{1,0,0}$を本社サーバ３－１－２に送信し、データ鍵$ｄｃ_{2,0,0}$を本社サーバ３－１－３に送信する。センターサーバ３－１－１は生成したデータ鍵$ｄｃ_{1,0,0}$及び$ｄｃ_{2,0,0}$を記憶装置に保持してもいいし、或いは、必要に応じて生成することとしてもよい。これにより、端末機器がデータ鍵$ｄｃ_{1,0,0}$及び$ｄｃ_{2,0,0}$を用いて暗号化した通信を復号することができる。
【０１０８】
また、鍵生成機能３－１－１－１は、予め生成したデータ鍵$ｄｃ_{1,0,0}$及び$ｄｃ_{2,0,0}$を用いて、必要に応じて或いは予め、支社サーバのデータ鍵を生成する。データ鍵を求めようとする支社サーバの上流に位置する本社サーバのデータ鍵と、その支社サーバの属性値$ＩＤ_{y}$をハッシュ演算する以下のような演算処理を実行することにより、所望の支社サーバのデータ鍵を算出する。
【０１０９】
支社サーバ３－１－４のデータ鍵$ｄｆ_{1,1,0}$：
$ｄｆ_{1,1,0}＝ｈ（ｄｃ_{1,0,0}||ＩＤ_{y1}）$
支社サーバ３－１－５のデータ鍵$ｄｆ_{1,2,0}$：
$ｄｆ_{1,2,0}＝ｈ（ｄｃ_{1,0,0}||ＩＤ_{y2}）$
支社サーバ３－１－６のデータ鍵$ｄｆ_{2,1,0}$：
$ｄｆ_{2,1,0}＝ｈ（ｄｃ_{2,0,0}||ＩＤ_{y1}）$
支社サーバ３－１－７のデータ鍵$ｄｆ_{2,2,0}$：
$ｄｆ_{2,2,0}＝ｈ（ｄｃ_{2,0,0}||ＩＤ_{y2}）$
【０１１０】
更に、鍵生成機能３－１－１－１は、予め生成したデータ鍵$ｄｆ_{1,1,0}$、$ｄｆ_{1,2,0}$、$ｄｆ_{2,1,0}$、$ｄｆ_{2,2,0}$と、グループ属性値$ＩＤ_{z}$を用いて、必要に応じて或いは予め、グループサーバのデータ鍵を生成する。データ鍵を求めようとするグループサーバの上流に位置する支社サーバのデータ鍵と、そのグループサーバの属性値$ＩＤ_{z}$をハッシュ演算する以下のような演算処理を実行することにより、所望のグループサーバのデータ鍵を算出する。
【０１１１】
グループサーバ３－１－８のデータ鍵$ｄｓ_{1,1,1}$：
$ｄｓ_{1,1,1}＝ｈ（ｄｆ_{1,1,0}||ＩＤ_{Z1}）$
グループサーバ３－１－９のデータ鍵$ｄｓ_{1,1,2}$：
$ｄｓ_{1,1,2}＝ｈ（ｄｆ_{1,1,0}||ＩＤ_{Z2}）$
グループサーバ３－１－１０のデータ鍵$ｄｓ_{1,2,1}$：
$ｄｓ_{1,2,1}＝ｈ（ｄｆ_{1,2,0}||ＩＤ_{Z1}）$
グループサーバ３－１－１１のデータ鍵$ｄｓ_{1,2,2}$：
$ｄｓ_{1,2,2}＝ｈ（ｄｆ_{1,2,0}||ＩＤ_{Z2}）$
グループサーバ３－１－１２のデータ鍵$ｄｓ_{2,1,1}$：
$ｄｓ_{2,1,1}＝ｈ（ｄｆ_{2,1,0}||ＩＤ_{Z1}）$
グループサーバ３－１－１３のデータ鍵$ｄｓ_{2,1,2}$：
$ｄｓ_{2,1,2}＝ｈ（ｄｆ_{2,1,0}||ＩＤ_{Z2}）$

グループサーバ３－１－１４のデータ鍵$ds_{2,2,1}$：
$ds_{2,2,1}=h(df_{2,2,0}||ID_{Z1})$
グループサーバ３－１－１５のデータ鍵$ds_{2,2,2}$：
$ds_{2,2,2}=h(df_{2,2,0}||ID_{Z2})$

【０１１２】

＜本社サーバの鍵生成機能３－１－２－１、３－１－３－１の動作＞

本社サーバ３－１－２において、鍵生成機能３－１－２－１は、センターサーバ３－１－１から受信したデータ鍵$dc_{1,0,0}$と、支社サーバの属性値ID_yを用いて、必要に応じて或いは予め、支社サーバ３－１－４、３－１－５のデータ鍵$df_{1,1,0}$、$df_{1,2,0}$を生成する。ここで実行される演算処理は、センターサーバ３－１－１において、鍵生成機能３－１－１－１がデータ鍵$df_{1,1,0}$、$df_{1,2,0}$を生成するために行う演算として既に説明したものと同じである。

【０１１３】

また、鍵生成機能３－１－４－１は、予め生成したデータ鍵$df_{1,1,0}$、$df_{1,2,0}$と、グループ属性値ID_zを用いて、必要に応じて或いは予め、グループサーバ３－１－８～３－１－１１のデータ鍵を生成する。ここで実行される演算処理は、センターサーバ３－１－１において、鍵生成機能３－１－１－１がデータ鍵$ds_{1,1,1}$、$ds_{1,1,2}$、$ds_{1,2,1}$、$ds_{1,2,2}$を生成するために行う演算として既に説明したものと同じである。

【０１１４】

他方、本社サーバ３－１－３において、鍵生成機能３－１－３－１は、上述の鍵生成機能３－１－２－１と同様に、センターサーバ３－１－１から受信したデータ鍵$dc_{2,0,0}$と、支社属性値ID_yを用いてデータ鍵$df_{2,1,0}$、$df_{2,2,0}$を生成する。更に、鍵生成機能３－１－３－１は、生成したデータ鍵$df_{2,1,0}$、$df_{2,2,0}$と、グループ属性値ID_zを用いてデータ鍵$ds_{2,1,1}$、$ds_{2,1,2}$、$ds_{2,2,1}$、$ds_{2,2,2}$を生成する。このとき鍵生成機能３－１－３－１が実行する演算処理は、鍵生成機能３－１－１－１が同じデータ鍵を生成する際に実行した既述の演算処理と同じである。

【０１１５】

＜支社サーバの鍵生成機能３－１－４－１～３－１－７－１の動作＞

支社サーバはいずれも上流にひとつの本社サーバが接続され、下流に２つのグループサーバが接続されている。支社サーバ３－１－４～３－１－７において、鍵生成機能３－１－４－１～３－１－７－１は、それぞれ、その支社サーバに接続された本社サーバから受信した自身のデータ鍵と、その支社サーバに接続されたグループサーバのグループ属性値ID_zとを用いて、必要に応じて或いは予め、グループサーバのデータ鍵を生成する。支社サーバは、生成する際に用いたグループ属性値を有するグループサーバに対してそのデータ鍵を送信する。

【０１１６】

支社サーバ３－１－４を例に挙げて説明する。支社サーバ３－１－４は、上流の本社サーバ３－１－２から自身のデータ鍵$df_{1,1,0}$を受信する。データ鍵$df_{1,1,0}$と、グループサーバ３－１－８のグループ属性値ID_{z1}とを連接したものをハッシュ演算することにより、支社サーバ３－１－４は、グループサーバ３－１－８のデータ鍵$ds_{1,1,1}$を生成する。このハッシュ演算は、センターサーバ３－１－１において鍵生成機能３－１－１－１がデータ鍵$ds_{1,1,1}$を生成する際に行うものと同じである。

【０１１７】

$ds_{1,1,1}=h(df_{1,1,0}||ID_{Z1})$

【０１１８】

支社サーバ３－１－４は生成したデータ鍵$ds_{1,1,1}$をグループサーバ３－１－８に送信する。また、支社サーバ３－１－４は、データ鍵$df_{1,1,0}$と、グループサーバ３－１－９のグループ属性値ID_{z2}とを連接したものをハッシュ演算することにより、

グループサーバ３－１－９のデータ鍵$ds_{1,1,2}$を生成する。このハッシュ演算は、鍵生成機能３－１－１－１がデータ鍵$ds_{1,1,2}$を生成する際に行うものと同じである。

【０１１９】

$ds_{1,1,2}=h(df_{1,1,0}||ID_{Z2})$

【０１２０】

支社サーバ３－１－４は生成したデータ鍵$ds_{1,1,2}$をグループサーバ３－１－９に送信する。

【０１２１】

同様に、支社サーバ３－１－５～３－１－７においても、その支社サーバの上流にある本社サーバから受け取った自身のデータ鍵と、生成しようとするデータ鍵の宛先となるグループサーバのグループ属性値ID_zとを連接したものをハッシュ演算することにより、その支社サーバの下流のグループサーバのデータ鍵を生成し、対応するグループサーバに送信する。

【０１２２】

支社サーバ３－１－５では鍵生成機能３－１－５－１にて次のハッシュ演算を行い、生成したデータ鍵$ds_{1,2,1}$をグループサーバ３－１－１０に送信する。

【０１２３】

$ds_{1,2,1}=h(df_{1,2,0}||ID_{Z1})$

【０１２４】

また、鍵生成機能３－１－５－１にて次のハッシュ演算を行い、生成したデータ鍵$ds_{1,2,2}$をグループサーバ３－１－１１に送信する。

【０１２５】

$ds_{1,2,2}=h(df_{1,2,0}||ID_{Z2})$

【０１２６】

支社サーバ３－１－６では鍵生成機能３－１－６－１にて次のハッシュ演算を行い、生成したデータ鍵$ds_{2,1,1}$をグループサーバ３－１－１２に送信する。

【０１２７】

$ds_{2,1,1}=h(df_{2,1,0}||ID_{Z1})$

【０１２８】

また、鍵生成機能３－１－６－１にて次のハッシュ演算を行い、生成したデータ鍵$ds_{2,1,2}$をグループサーバ３－１－１３に送信する。

【０１２９】

$ds_{2,1,2}=h(df_{2,1,0}||ID_{Z2})$

【０１３０】

支社サーバ３－１－７では鍵生成機能３－１－７－１にて次のハッシュ演算を行い、生成したデータ鍵$ds_{2,2,1}$をグループサーバ３－１－１４に送信する。

【０１３１】

$ds_{2,2,1}=h(df_{2,2,0}||ID_{Z1})$

【０１３２】

また、鍵生成機能３－１－７－１にて次のハッシュ演算を行い、生成したデータ鍵$ds_{2,2,2}$をグループサーバ３－１－１５に送信する。

【０１３３】

$ds_{2,2,2}=h(df_{2,2,0}||ID_{Z2})$

【０１３４】

上記サーバー間でのデータ鍵の受け渡しは事前に用意されたデータ鍵受け渡し用の暗号鍵で暗号化して行われる。

【０１３５】

＜端末機器の鍵生成機能３－２－１－１～３－２－３２－１の動作＞

図１３～２０に示した手順により、端末機器３－２－１～３－２－３２には、接続され

たグループサーバと同じ属性値（ID_x，ID_y，ID_z）が図２１に示すように設定されている。本実施例では、８つのグループサーバそれぞれの配下に４つの端末機器が接続されているので、属性値が同じ端末機器が４台ずつ存在する。

【０１３６】

端末機器は自身に設定された属性値から、自身が属する本社サーバの本社属性値、支社サーバの支社属性値、グループサーバのグループ属性値を取得することができる。各端末機器の鍵生成機能は、自身に設定された属性値と、別途通知される秘密シードｓとを元に、自身の上流にある本社サーバ、支社サーバ、グループサーバと通信するためのデータ鍵を生成する。秘密シードｓと本社属性値ID_xとを連接した値をハッシュ演算して本社サーバのデータ鍵dc_{xyz}を生成し、生成したデータ鍵dc_{xyz}と支社属性値ID_yとを連接した値をハッシュ演算して支社サーバのデータ鍵df_{xyz}を生成し、生成したデータ鍵df_{xyz}とグループ属性値ID_zとを連接した値をハッシュ演算してグループサーバのデータ鍵ds_{xyz}を生成する。同一グループサーバ配下にある端末機器のデータ鍵dc_{xyz}、df_{xyz}、ds_{xyz}は共通である。

【０１３７】

例えば、端末機器３－２－１～３－２－４の鍵生成機能３－２－１－１～３－２－４－１は、必要に応じて或いは予め、次の４つのハッシュ演算を行うことにより、本社サーバ３－１－２のデータ鍵$dc_{1,0,0}$、支社サーバ３－１－４のデータ鍵$df_{1,1,0}$、グループサーバ３－１－８のデータ鍵$ds_{1,1,1}$を生成する。

【０１３８】

$dc_{1,0,0}=h(s||ID_{X1})$
$df_{1,1,0}=h(dc_{1,0,0}||ID_{y1})$
$ds_{1,1,1}=h(df_{1,1,0}||ID_{Z1})$

【０１３９】

また、例えば、端末機器３－２－５～３－２－８の鍵生成機能３－２－５－１～３－２－８－１は、必要に応じて或いは予め、次の４つのハッシュ演算を行うことにより、本社サーバ３－１－２のデータ鍵$dc_{1,0,0}$、支社サーバ３－１－４のデータ鍵$df_{1,1,0}$、グループサーバ３－１－９のデータ鍵$ds_{1,1,2}$を生成する。

【０１４０】

$dc_{1,0,0}=h(s||ID_{X1})$
$df_{1,1,0}=h(dc_{1,0,0}||ID_{y1})$
$ds_{1,1,2}=h(df_{1,1,0}||ID_{Z2})$

【０１４１】

別の例としては、端末機器３－２－２９～３－２－３２の鍵生成機能３－２－２９－１～３－２－３２－１は、必要に応じて或いは予め、次の４つのハッシュ演算を行うことにより、本社サーバ３－１－３のデータ鍵$dc_{2,0,0}$、支社サーバ３－１－７のデータ鍵$df_{2,2,0}$、グループサーバ３－１－１５のデータ鍵$ds_{2,2,2}$を生成する。

【０１４２】

$dc_{2,0,0}=h(s||ID_{X2})$
$df_{2,2,0}=h(dc_{2,0,0}||ID_{y2})$
$ds_{2,2,2}=h(df_{2,2,0}||ID_{Z2})$

【０１４３】

＜暗号通信＞

実施例１では、各端末機器は４つのデータ鍵、即ち、自身を配下とするセンターサーバ、本社サーバ、支社サーバ、グループサーバの４種類のサーバそれぞれと暗号通信を行うためのデータ鍵を生成したが、これら４種類のサーバでは自身の直下にあるサーバのデータ鍵のみを生成して暗号通信を行った。例えば、センターサーバ２－１－１は本社サーバ２－１－２、２－１－３のデータ鍵を生成するが、支社サーバ２－１－４～２－１－７、グループサーバ２－１－８～２－１－１５のデータ鍵は生成しなかった。

【０１４４】

これに対して、本実施例では、各サーバの鍵生成機能は、自身の直下にあるサーバだけではなく、そのサーバの更に下流にあるサーバのデータ鍵も生成する。例えば、ネットワークシステムの最上位にあるセンターサーバ３－１－１では全てのサーバのデータ鍵を生成する。また、本社サーバ３－１－２では直下にある、本社サーバ３－１－１を親とすればいわば子に相当する関係にある支社サーバ３－１－４、３－１－５だけではなく、孫に相当するグループサーバ３－１－８～３－１－１１のデータ鍵についても生成する。これにより、図４に示すような暗号通信の可否の関係を構築する。

【０１４５】

例えば、端末機器３－２－１は秘密シードｓ、データ鍵$dc_{1,0,0}$、$df_{1,1,0}$、$ds_{1,1,1}$を用いて暗号通信を行うことができるが、秘密シードｓを用いて暗号化した場合、復号に必要な鍵である秘密シードｓを有するのはセンターサーバ３－１－１のみであり、他のサーバは鍵を保持していないため復号できない。本社サーバ３－１－２のデータ鍵$dc_{1,0,0}$にて暗号化した暗号通信の場合、本社サーバ３－１－２とその上位にあるセンターサーバ３－１－１はデータ鍵$dc_{1,0,0}$を生成可能であり復号可能であるが、他のサーバでは生成できず復号できない。

【０１４６】

以上、本発明を実施の形態及び実施例に即して説明したが、本発明はこれに限定されるものではなく、発明の技術的範囲内で様々な変形が可能であることは当業者には明らかであろう。

【０１４７】

例えば、属性値とは別に端末機器に付与される固有ＩＤを用いて、センターサーバが特定の端末機器と暗号通信を行うことが考えられる。手順は例えば次の通りである。

【０１４８】

（１）センターサーバは、暗号通信しようとする端末機器からその端末機器の固有ＩＤを取得する。

【０１４９】

（２）センターサーバは、その固有ＩＤと秘密シードｓとを連接し、それをハッシュして暗号鍵dk_iを生成する。

【０１５０】

（３）センターサーバは暗号鍵dk_iを用いて通信文を暗号化してその特定の端末機器に送信する。

【０１５１】

（４）センターサーバから暗号文を受信した端末機器は、自身の固有ＩＤと予め通知されている秘密シードｓとを連接し、それをハッシュして暗号鍵dk_iを生成する。

【０１５２】

（５）端末機器は自身で生成した暗号鍵dk_iを用いて暗号文を復号する。

【０１５３】

上述したデータ鍵による暗号通信では、センターサーバと、一のグループサーバ配下の複数の端末機器との間での暗号通信を行うものであり、いわば一対多の暗号通信であったが、ここで述べたような暗号鍵dk_iによる暗号通信を併用することにより、センターサーバと特定の端末装置との間の暗号通信をも可能とすることができる。尚、この例ではセンターサーバと端末機器の間の個別暗号鍵での暗号通信を示したが、本社サーバと端末機器、支社サーバと端末機器、グループサーバと端末機器の各々の間でも同様に各サーバの暗号鍵と端末機器の個有ＩＤを用い個別の暗号通信を行うことが出来る。

【符号の説明】

【０１５４】

１００　ネットワークシステム

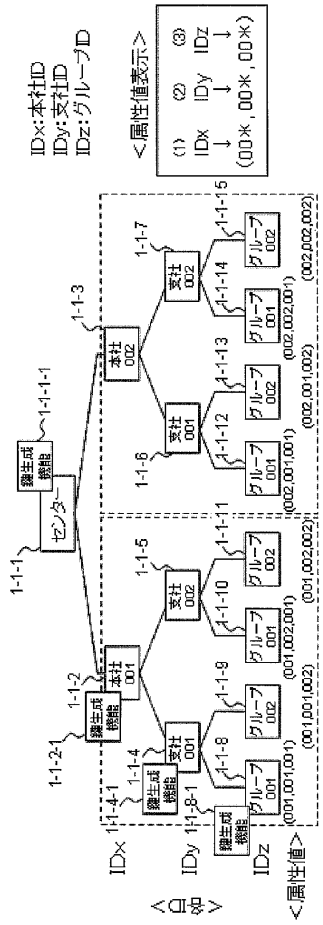
１－１－１、２－１－１、３－１－１　センターサーバ

１－１－２、１－１－３、２－１－２、２－１－３　本社サーバ

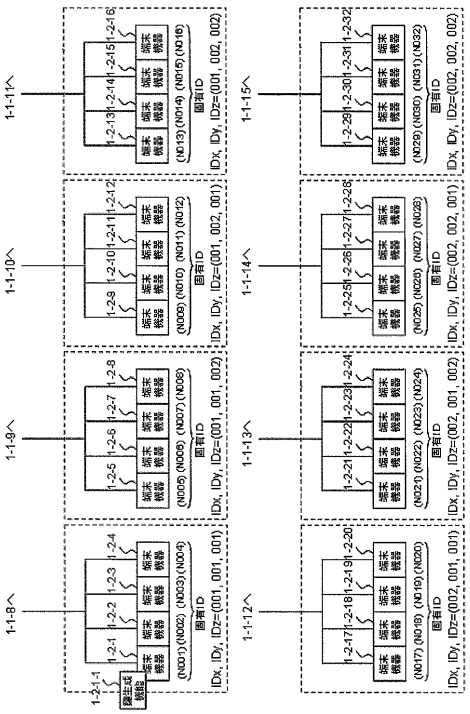
１－１－４～１－１－７、２－１－４～２－１－７、３－１－４～３－１－７　支社サー

バ
１－１－８～１－１－１５、２－１－８～２－１－１５、３－１－８～３－１－１５　グループサーバ
１－１－１－１、１－１－２－１、１－１－４－１、１－１－８－１、１－２－１－１、２－１－１－１、２－１－２－１、２－１－４－１、２－１－８－１、２－２－１－１、３－１－１－１、３－１－２－１、３－１－４－１、３－１－８－１、３－２－１－１　鍵生成機能
１－２－１～１－２－３２、２－２－１～２－２－３２、３－２－１～３－２－３２　端末機器
１－３－７、１－３－８、１－３－９、１－３－１０　データ鍵

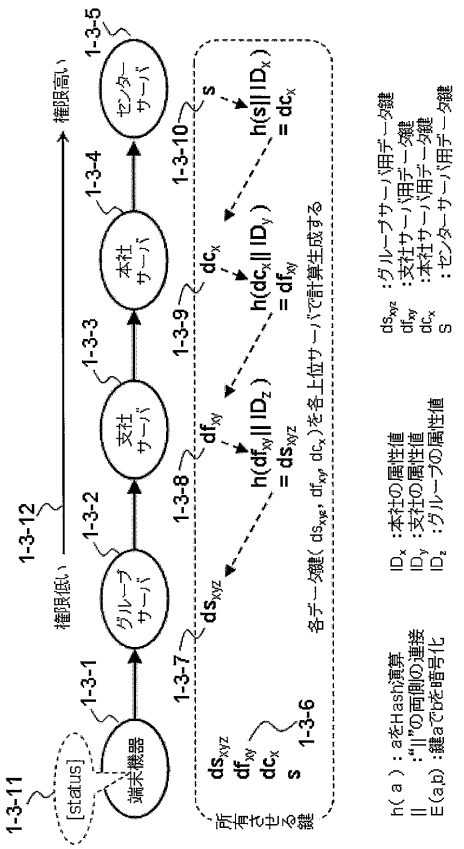
【図１】



【図２】



【図３】

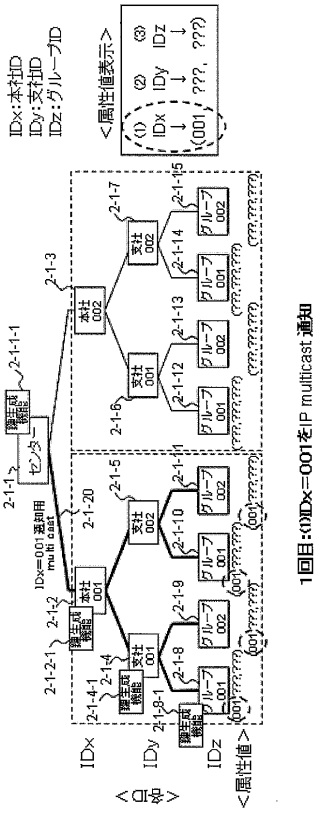


【図４】

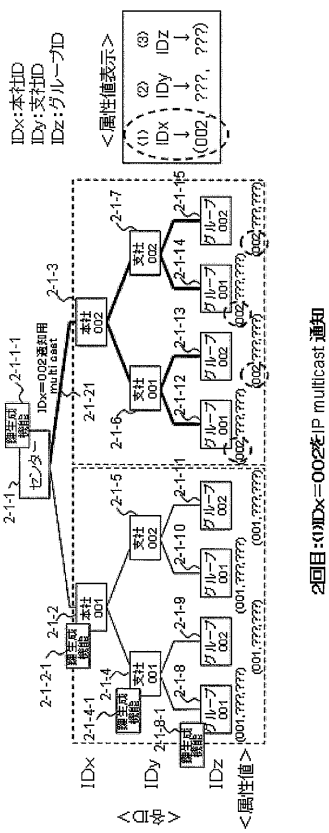
	端末機器との間で暗号通信が可能(○)／不可能(×)			
暗号化情報	グループサーバ	支社サーバ	本社サーバ	センターサーバ
$E(ds_{xyz}, [status])$	○	○	○	○
$E(df_{xy}, [status])$	×	○	○	○
$E(dc_x, [status])$	×	×	○	○
$E(s, [status])$	×	×	×	○

E(a, b): 鍵aでbを暗号化
ds_{xyz}: グループサーバ用データ鍵
df_{xy}: 支社サーバ用データ鍵
dc_x: 本社サーバ用データ鍵
s: センターサーバ用データ鍵(秘密シード)

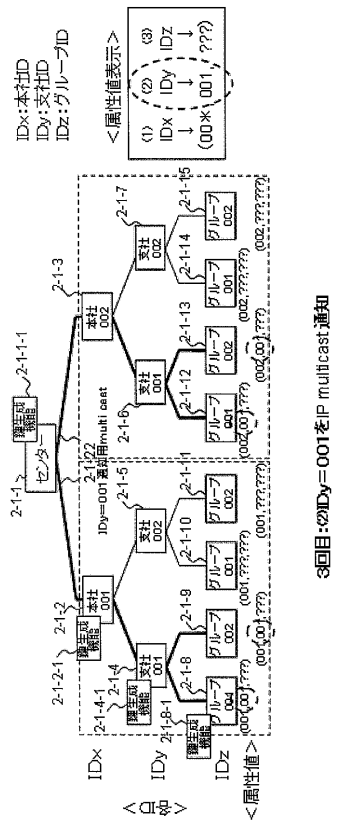
【図５】



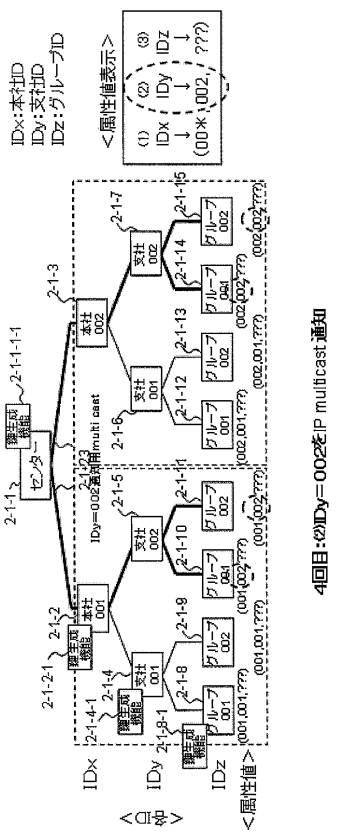
【図６】



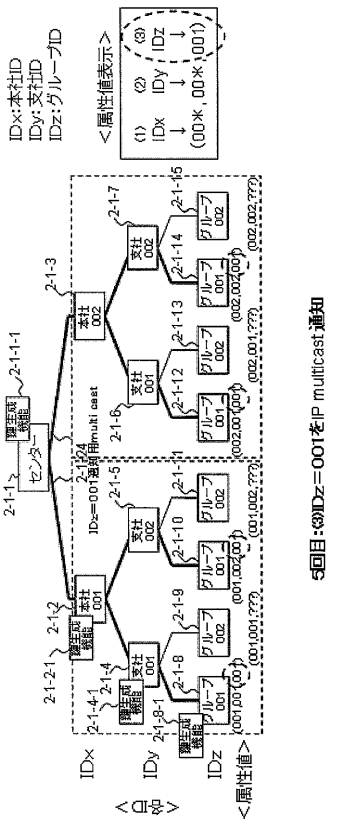
【図７】


IDx:本社ID
IDy:支社ID
IDz:グループID
<属性値表示>
(1) IDx → (2) IDy → (3) IDz
(00*, 001, ???)
センタ
2-1-1
2-1-1-1
2-1-2
2-1-3
2-1-4
2-1-5
2-1-6
2-1-7
2-1-8
2-1-9
2-1-10
2-1-11
2-1-12
2-1-13
2-1-14
2-1-15
2-1-2-1
2-1-4-1
2-1-8-1
IDy=001宛用multi cast
本社 001
本社 002
支社 001
支社 002
グループ 001
グループ 002
IDx
IDy
IDz
<ロール>
<属性値>
3回目:②IDy=001をIP multicast通知

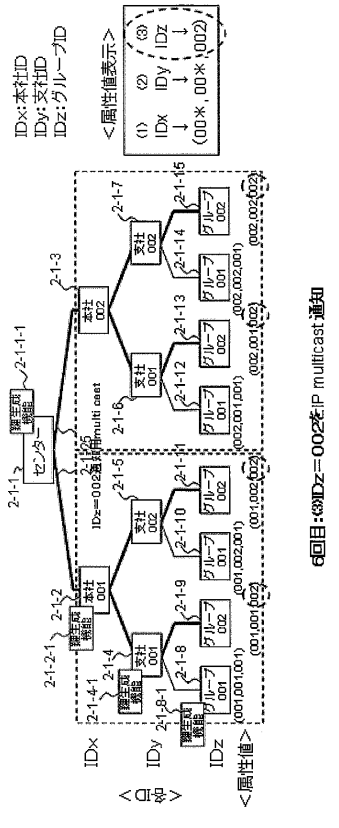
【図８】


IDx:本社ID
IDy:支社ID
IDz:グループID
<属性値表示>
(1) IDx → (2) IDy → (3) IDz
(00*, 002, ???)
センタ
2-1-1
2-1-1-1
2-1-2
2-1-3
2-1-4
2-1-5
2-1-6
2-1-7
2-1-8
2-1-9
2-1-10
2-1-11
2-1-12
2-1-13
2-1-14
2-1-15
2-1-2-1
2-1-4-1
2-1-8-1
IDy=002宛用multi cast
本社 001
本社 002
支社 001
支社 002
グループ 001
グループ 002
IDx
IDy
IDz
<ロール>
<属性値>
4回目:②IDy=002をIP multicast通知

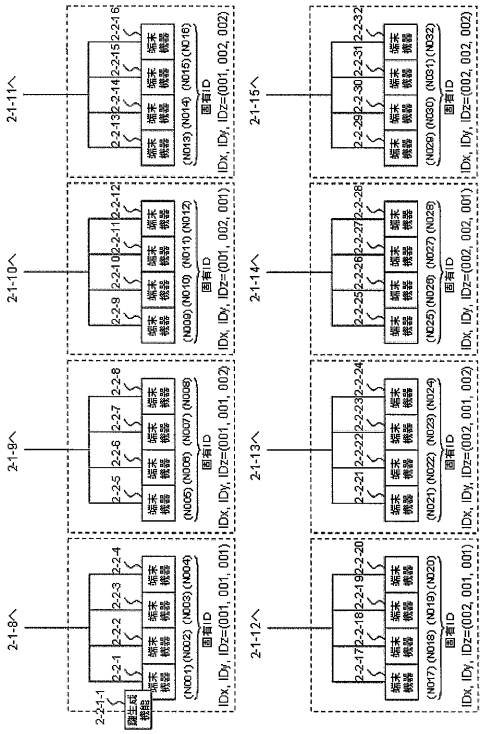
【図９】


IDx:本社ID
IDy:支社ID
IDz:グループID
<属性値表示>
(1) IDx → (2) IDy → (3) IDz
(00*, 00*, 001)
センタ
2-1-1
2-1-1-1
2-1-2
2-1-3
2-1-4
2-1-5
2-1-6
2-1-7
2-1-8
2-1-9
2-1-10
2-1-11
2-1-12
2-1-13
2-1-14
2-1-15
2-1-2-1
2-1-4-1
2-1-8-1
IDz=001宛用multi cast
本社 001
本社 002
支社 001
支社 002
グループ 001
グループ 002
IDx
IDy
IDz
<ロール>
<属性値>
5回目:③IDz=001をIP multicast通知

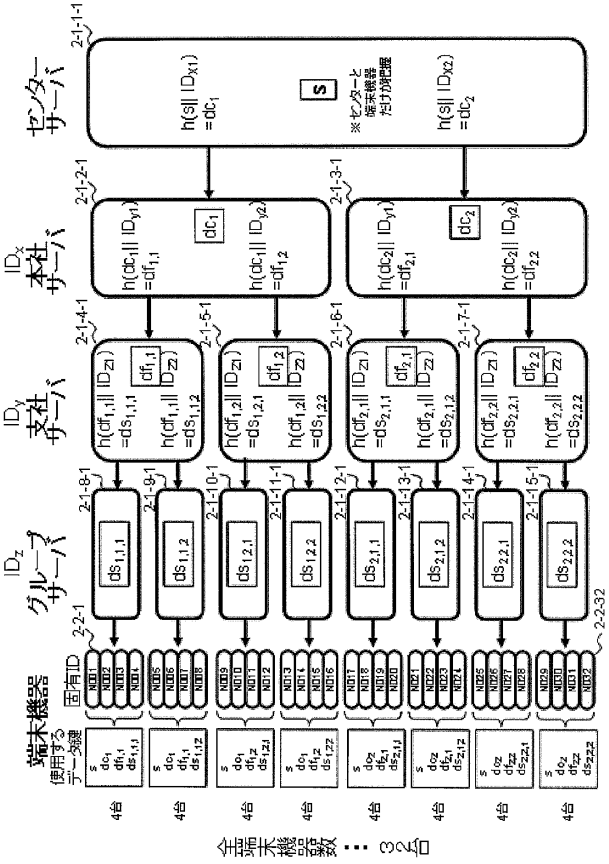
【図１０】


IDx:本社ID
IDy:支社ID
IDz:グループID
<属性値表示>
(1) IDx → (2) IDy → (3) IDz
(00*, 00*, 002)
センタ
2-1-1
2-1-1-1
2-1-2
2-1-3
2-1-4
2-1-5
2-1-6
2-1-7
2-1-8
2-1-9
2-1-10
2-1-11
2-1-12
2-1-13
2-1-14
2-1-15
2-1-2-1
2-1-4-1
2-1-8-1
IDz=002宛用multi cast
本社 001
本社 002
支社 001
支社 002
グループ 001
グループ 002
IDx
IDy
IDz
<ロール>
<属性値>
6回目:③IDz=002をIP multicast通知

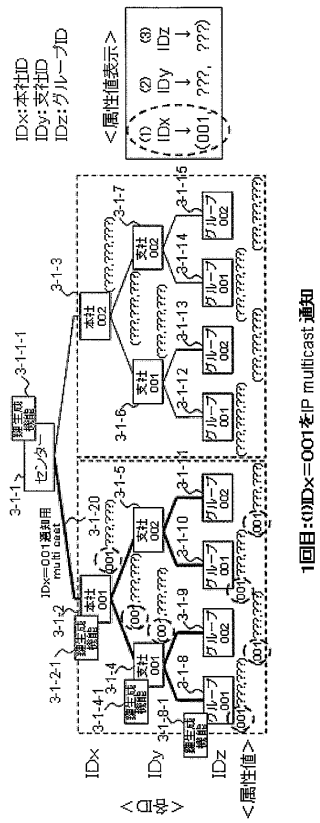
【図１１】



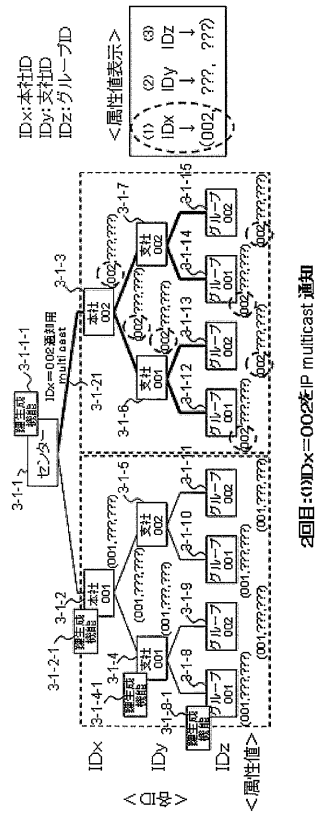
【図１２】



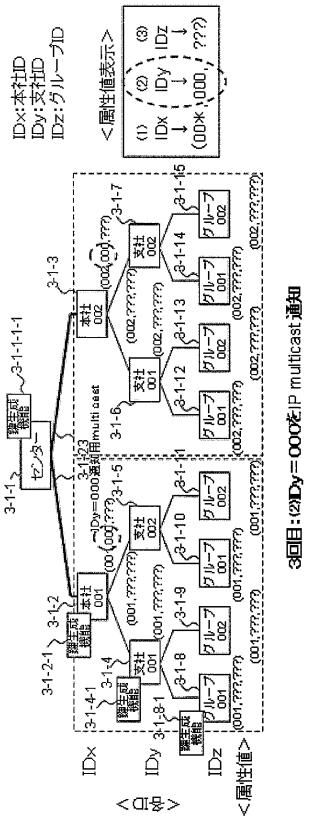
【図１３】



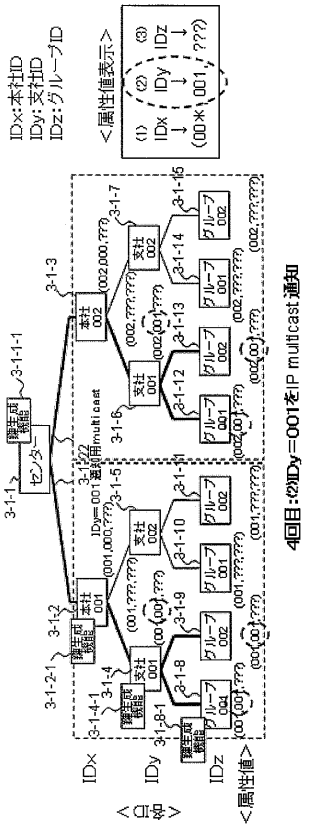
【図１４】



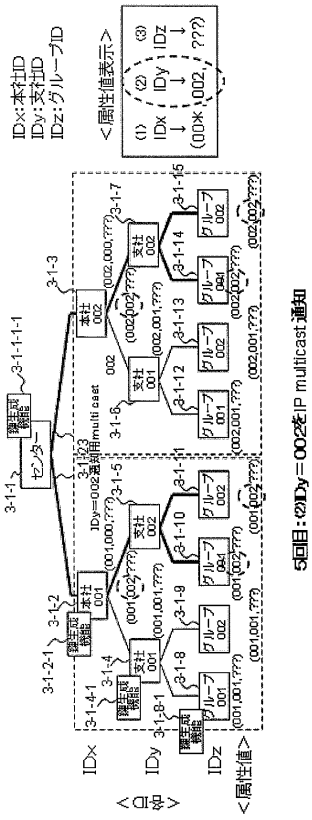
【図１５】



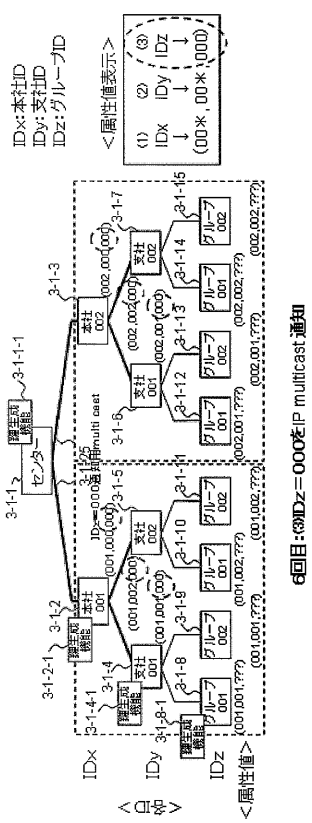
【図１６】



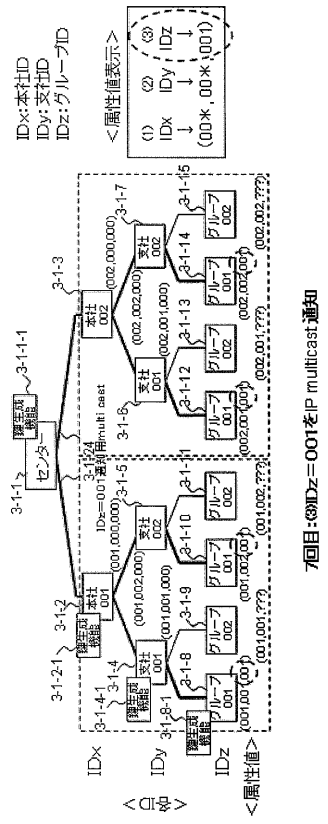
【図１７】



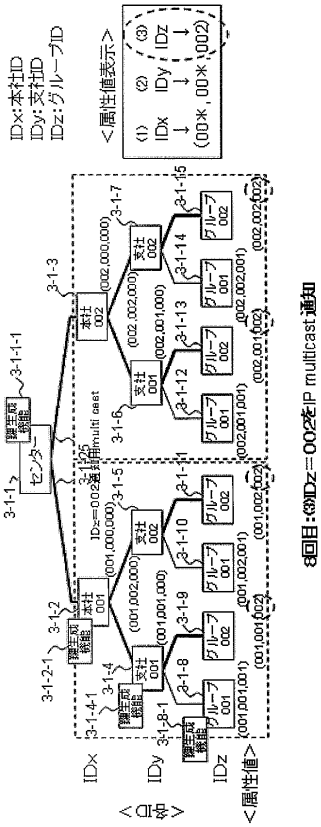
【図１８】



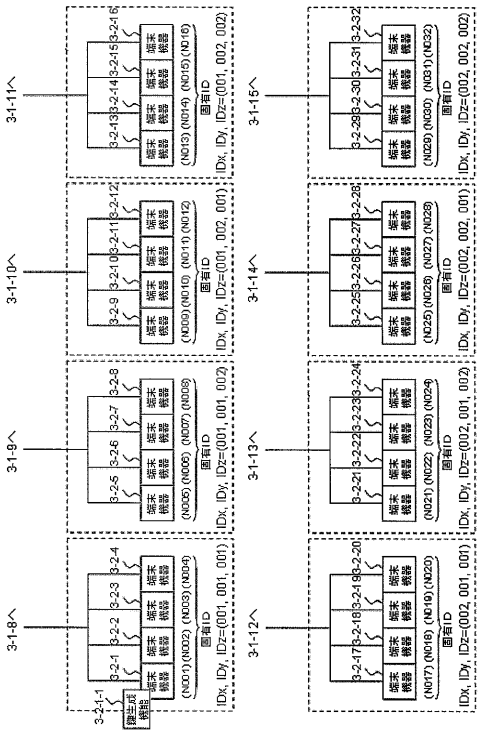
【図１９】



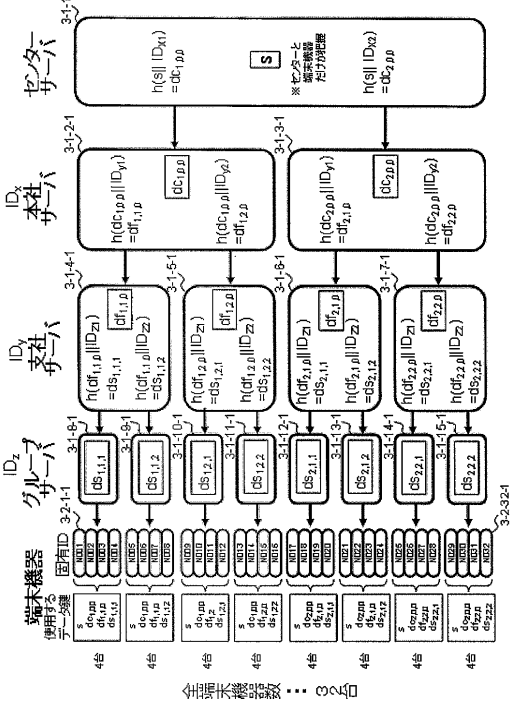
【図２０】



【図２１】



【図２２】



フロントページの続き

(72)発明者　伊藤　隆司
東京都千代田区一ツ橋２丁目６番３号　株式会社エルイーテック内
(72)発明者　小泉　達也
東京都千代田区一ツ橋２丁目６番３号　株式会社エルイーテック内
(72)発明者　石井　豊和
東京都千代田区一ツ橋２丁目６番３号　株式会社エルイーテック内

Ｆターム(参考) 5J104 AA16　EA07　EA16　JA03　NA02　NA12　NA36　NA37　PA07