(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4823717号
(P4823717)

(45)発行日　平成23年11月24日(2011.11.24)　(24)登録日　平成23年9月16日(2011.9.16)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601B
G06F 21/20 (2006.01)　　H04L 9/00 601E
　　G06F 15/00 330A

請求項の数 11　(全 34 頁)

(21)出願番号　特願2006-52361 (P2006-52361)
(22)出願日　平成18年2月28日 (2006.2.28)
(65)公開番号　特開2007-235348 (P2007-235348A)
(43)公開日　平成19年9月13日 (2007.9.13)
審査請求日　平成20年8月15日 (2008.8.15)

（出願人による申告）国等の委託研究の成果に係る特許出願（平成１７年度総務省「認証機能を具備するサービスプラットフォーム技術」委託研究、産業活力再生特別措置法第３０条の適用を受けるもの）

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　高田　治
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　鍛　忠司
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】暗号通信システム、端末状態管理サーバ、暗号通信方法、および端末状態管理方法

(57)【特許請求の範囲】
【請求項１】
セッション管理サーバによって生成された鍵情報を用いて、複数の通信端末で構成されるグループ内で行われるグループ内暗号通信を実現する暗号通信システムであって、
それぞれの前記通信端末に関する情報を格納するデータベースと、
前記複数の通信端末によって実行されるグループ内暗号通信を管理する端末状態管理サーバと
を備え、
前記データベースは、
前記通信端末を識別する端末ＩＤに対応付けて、前記グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納する参加端末アドレス格納手段と、
前記複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納するグループメンバ情報格納手段と
を有し、
前記端末状態管理サーバは、
グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づき前記グループメンバ格納手段を参照して、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出手段と、
前記参加端末アドレス格納手段を参照して、前記グループメンバ抽出手段によって抽出

された端末ＩＤの中から、端末アドレスに対応付けられて前記参加端末アドレス格納手段内に格納されている端末ＩＤを抽出して、前記セッション管理サーバへ出力することにより、前記セッション管理サーバに、前記グループ内暗号通信要求に含まれるグループＩＤに対応するグループ内の参加端末のそれぞれへ、当該グループ内でのグループ内暗号通信に用いる鍵情報を配布させる参加端末ＩＤ抽出手段と
を有することを特徴とする暗号通信システム。

【請求項２】

請求項１に記載の暗号通信システムであって、
前記セッション管理サーバをさらに備え、
前記セッション管理サーバは、
前記通信端末から、前記グループ内暗号通信に参加する旨を通知された場合に、当該通信端末の端末アドレスを参加端末の端末アドレスとして、端末ＩＤに対応付けて前記参加端末アドレス格納手段に格納する参加端末登録手段を有することを特徴とする暗号通信システム。

【請求項３】

請求項２に記載の暗号通信システムであって、
前記セッション管理サーバは、
前記通信端末との間で暗号通信路を確立し、確立した暗号通信路を介して、当該通信端末とデータを送受信する暗号通信手段をさらに有し、
前記グループメンバ抽出手段は、
前記暗号通信路を介して、前記通信端末から前記グループ内暗号通信要求を受信し、
前記データベースサーバは、
前記参加端末のそれぞれがグループ内暗号通信において実行可能な１つ以上の通信条件を、前記端末ＩＤに対応付けて格納する通信条件格納手段をさらに有し、
前記セッション管理サーバは、
前記参加端末ＩＤ抽出手段から出力された端末ＩＤを受信し、受信した端末ＩＤのそれぞれに対応付けられている通信条件を前記通信条件格納手段から抽出し、抽出した通信条件の中から複数の端末ＩＤに共通の通信条件を抽出し、抽出した通信条件において実行可能なグループ内暗号通信に用いられる鍵情報を生成し、生成した鍵情報を、前記参加端末ＩＤ抽出手段から受信した端末ＩＤに対応する通信端末のそれぞれへ、前記暗号通信路を介して送信する鍵生成配布手段をさらに有することを特徴とする暗号通信システム。

【請求項４】

請求項３に記載の暗号通信システムであって、
前記鍵生成配布手段は、
生成した鍵情報と共に、前記参加端末ＩＤ抽出手段から受信した端末ＩＤの一覧を、当該端末ＩＤに対応する通信端末のそれぞれへさらに配布することを特徴とする暗号通信システム。

【請求項５】

請求項３に記載の暗号通信システムであって、
前記データベースは、
グループに対応するマルチキャストアドレスまたはブロードキャストであるグループアドレスを当該グループのグループＩＤに対応付けて格納するグループアドレス格納手段をさらに備え、
前記グループメンバ抽出手段は、
前記グループ内暗号通信要求を受信した場合に、当該グループ内暗号通信要求に含まれるグループＩＤに基づいて前記グループアドレス格納手段を参照して、当該グループＩＤに対応するグループアドレスをさらに抽出し、
前記参加端末ＩＤ抽出手段は、
抽出した端末ＩＤと共に、前記グループメンバ抽出手段によって抽出されたグループアドレスをさらに出力し、

前記鍵生成手段は、
生成した鍵情報と共に、前記参加端末ＩＤ抽出手段から受信したグループアドレスを、対応する通信端末のそれぞれへ、前記暗号通信路を介して送信することを特徴とする暗号通信システム。
【請求項６】
請求項１に記載の暗号通信システムであって、
前記グループ内暗号通信要求には、当該グループ内暗号通信要求の送信元の通信端末の端末ＩＤがさらに含まれ、
前記グループメンバ抽出手段は、
前記グループメンバ格納手段を参照して、受信したグループ内暗号通信要求に含まれるグループＩＤに属する通信端末の端末ＩＤの中に、当該グループ内暗号通信要求に含まれる端末ＩＤが含まれている場合に、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出することを特徴とする暗号通信システム。
【請求項７】
複数の通信端末で構成されるグループ内の暗号通信であるグループ内暗号通信を実現する暗号通信システムであって、
それぞれの前記通信端末に関する情報を格納するデータベースと、
前記複数の通信端末によって実行されるグループ内暗号通信を管理する端末状態管理サーバと、
前記グループ内暗号通信に用いられる鍵情報を生成してそれぞれの前記通信端末へ配布するセッション管理サーバと、
複数の通信端末と
を備え、
前記データベースは、
前記通信端末を識別する端末ＩＤに対応付けて、前記グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納する参加端末アドレス格納手段と、
前記複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納するグループメンバ情報格納手段と、
前記参加端末のそれぞれがグループ内暗号通信において実行可能な１つ以上の通信条件を、前記端末ＩＤに対応付けて格納する通信条件格納手段と
を有し、
前記端末状態管理サーバは、
前記セッション管理サーバを介して、グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づいて前記グループメンバ格納手段を参照して、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出手段と、
前記参加端末アドレス格納手段を参照して、前記グループメンバ抽出手段によって抽出された端末ＩＤの中から、端末アドレスに対応付けられて前記参加端末アドレス格納手段内に格納されている端末ＩＤを抽出して、前記セッション管理サーバへ出力する参加端末ＩＤ抽出手段と
を有し、
前記セッション管理サーバは、
前記通信端末との間で暗号通信路を確立し、確立した暗号通信路を介して、当該通信端末とデータを送受信するサーバ側暗号通信手段と、
前記通信端末から、前記暗号通信路を介して、前記グループ内暗号通信に参加する旨を通知された場合に、当該通信端末の端末アドレスを参加端末の端末アドレスとして、端末ＩＤに対応付けて前記参加端末アドレス格納手段に格納する参加端末登録手段と、
前記参加端末ＩＤ抽出手段から出力された端末ＩＤを受信し、受信した端末ＩＤのそれぞれに対応付けられている通信条件を前記通信条件格納手段から抽出し、抽出した通信条

件の中から複数の端末ＩＤに共通の通信条件を抽出し、抽出した通信条件において実行可能なグループ内暗号通信に用いられる前記鍵情報を生成し、生成した鍵情報を、前記参加端末ＩＤ抽出手段から受信した端末ＩＤに対応する通信端末のそれぞれへ、前記暗号通信路を介して送信する鍵生成配布手段と
を有し、
前記複数の通信端末のそれぞれは、
前記セッション管理サーバとの間で暗号通信路を確立し、確立した暗号通信路を介して、当該セッション管理サーバとデータを送受信する端末側暗号通信手段と、
前記グループ内暗号通信を開始する場合に、前記グループ内暗号通信要求を、前記暗号通信路を介して前記セッション管理サーバへ送信する暗号通信要求手段と、
前記セッション管理サーバから、前記グループ内暗号通信要求に応答して、前記鍵情報を前記暗号通信路を介して受信した場合に、当該鍵情報を用いてグループ内の他の通信端末との間でグループ内暗号通信を実行するグループ内暗号通信手段と
を有することを特徴とする暗号通信システム。

【請求項８】
セッション管理サーバによって生成された鍵情報を用いて、複数の通信端末で構成されるグループ内で行われるグループ内暗号通信を実現する暗号通信システムにおいて、記憶装置に格納された情報を用いて鍵情報の配布を前記セッション管理サーバに指示する端末状態管理サーバであって、
グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づいて前記記憶装置を参照し、前記複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納している、前記記憶装置内のグループメンバ情報格納手段から、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出手段と、
前記通信端末を識別する端末ＩＤに対応付けて、前記グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納している、前記記憶装置内の参加端末アドレス格納手段を参照して、前記グループメンバ抽出手段によって抽出された端末ＩＤの中から、端末アドレスに対応付けられて前記参加端末アドレス格納手段内に格納されている端末ＩＤを抽出して前記セッション管理サーバへ出力することにより、前記セッション管理サーバに、前記グループ内暗号通信要求に含まれるグループＩＤに対応するグループ内の参加端末のそれぞれへ、当該グループ内でのグループ内暗号通信に用いる鍵情報を配布させる参加端末ＩＤ抽出手段と
を備えることを特徴とする端末状態管理サーバ。

【請求項９】
セッション管理サーバによって生成された鍵情報を用いて、複数の通信端末で構成されるグループ内で行われるグループ内暗号通信を実現する暗号通信システムにおける暗号通信方法であって、
前記暗号通信システムは、
それぞれの前記通信端末に関する情報を格納するデータベースと、
前記複数の通信端末によって実行されるグループ内暗号通信を管理する端末状態管理サーバと
を備え、
前記データベースは、
前記通信端末を識別する端末ＩＤに対応付けて、前記グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納する参加端末アドレス格納手段と、
前記複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納するグループメンバ情報格納手段と
を有し、
前記端末状態管理サーバは、

グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づいて前記グループメンバ格納手段を参照して、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出ステップと、
前記参加端末アドレス格納手段を参照して、前記グループメンバ抽出ステップにおいて抽出した端末ＩＤの中から、端末アドレスに対応付けられて前記参加端末アドレス格納手段内に格納されている端末ＩＤを抽出して前記セッション管理サーバへ出力することにより、前記グループ内暗号通信要求に含まれるグループＩＤに対応するグループ内の参加端末のそれぞれへ、当該グループ内でのグループ内暗号通信に用いる鍵情報を生成して配布させる参加端末ＩＤ抽出ステップと
を実行することを特徴とする暗号通信方法。

【請求項１０】
複数の通信端末で構成されるグループ内の暗号通信であるグループ内暗号通信を実現する暗号通信システムにおける暗号通信方法であって、
前記暗号通信システムは、
それぞれの前記通信端末に関する情報を格納するデータベースと、
前記複数の通信端末によって実行されるグループ内暗号通信を管理する端末状態管理サーバと、
前記グループ内暗号通信に用いられる鍵情報を生成してそれぞれの前記通信端末へ配布するセッション管理サーバと、
複数の通信端末と
を備え、
前記データベースは、
前記通信端末を識別する端末ＩＤに対応付けて、前記グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納する参加端末アドレス格納手段と、
前記複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納するグループメンバ情報格納手段と、
前記参加端末のそれぞれがグループ内暗号通信において実行可能な１つ以上の通信条件を、前記端末ＩＤに対応付けて格納する通信条件格納手段と
を有し、
前記端末状態管理サーバは、
前記セッション管理サーバを介して、グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づいて前記グループメンバ格納手段を参照して、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出ステップと、
前記参加端末アドレス格納手段を参照して、前記グループメンバ抽出ステップにおいて抽出した端末ＩＤの中から、端末アドレスに対応付けられて前記参加端末アドレス格納手段内に格納されている端末ＩＤを抽出して、前記セッション管理サーバへ出力する参加端末ＩＤ抽出ステップと
を行い、
前記セッション管理サーバは、
前記通信端末との間で暗号通信路を確立し、確立した暗号通信路を介して、当該通信端末とデータを送受信するサーバ側暗号通信ステップと、
前記通信端末から、前記暗号通信路を介して、前記グループ内暗号通信に参加する旨を通知された場合に、当該通信端末の端末アドレスを参加端末の端末アドレスとして、端末ＩＤに対応付けて前記参加端末アドレス格納手段に格納する参加端末登録ステップと、
前記参加端末ＩＤ抽出ステップにおいて出力された端末ＩＤを受信し、受信した端末ＩＤのそれぞれに対応付けられている通信条件を前記通信条件格納手段から抽出し、抽出した通信条件の中から複数の端末ＩＤに共通の通信条件を抽出し、抽出した通信条件において実行可能なグループ内暗号通信に用いられる前記鍵情報を生成し、生成した鍵情報を、

前記参加端末ＩＤ抽出ステップにおいて出力された端末ＩＤに対応する通信端末のそれぞれへ、前記暗号通信路を介して送信する鍵生成配布ステップと
を行い、
前記複数の通信端末のそれぞれは、
前記セッション管理サーバとの間で暗号通信路を確立し、確立した暗号通信路を介して、当該セッション管理サーバとデータを送受信する端末側暗号通信ステップと、
前記グループ内暗号通信を開始する場合に、前記グループ内暗号通信要求を、前記暗号通信路を介して前記セッション管理サーバへ送信する暗号通信要求ステップと、
前記セッション管理サーバから、前記グループ内暗号通信要求に応答して、前記鍵情報を前記暗号通信路を介して受信した場合に、当該鍵情報を用いてグループ内の他の通信端末との間でグループ内暗号通信を実行するグループ内暗号通信ステップと
を実行することを特徴とする暗号通信方法。
【請求項１１】
セッション管理サーバによって生成された鍵情報を用いて、複数の通信端末で構成されるグループ内で行われるグループ内暗号通信を実現する暗号通信システムにおいて、記憶装置に格納された情報を用いて鍵情報の生成を前記セッション管理サーバに指示する端末状態管理サーバにおける端末状態管理方法であって、
前記端末状態管理サーバは、
グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づいて前記記憶装置を参照し、前記複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納している、前記記憶装置内のグループメンバ情報格納手段から、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出ステップと、
前記通信端末を識別する端末ＩＤに対応付けて、前記グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納している、前記記憶装置内の参加端末アドレス格納手段を参照して、前記グループメンバ抽出ステップにおいて抽出した端末ＩＤの中から、端末アドレスに対応付けられて前記参加端末アドレス格納手段内に格納されている端末ＩＤを抽出して前記セッション管理サーバへ出力することにより、前記セッション管理サーバに、前記グループ内暗号通信要求に含まれるグループＩＤに対応するグループ内の参加端末のそれぞれへ、当該グループ内でのグループ内暗号通信に用いる鍵情報を配布させる参加端末ＩＤ抽出ステップと
を行うことを特徴とする端末状態管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号通信技術に関し、特に複数の通信端末で構成されるグループ内の暗号通信に用いられる暗号鍵を、当該通信端末のそれぞれに配布する技術に関する。
【背景技術】
【０００２】
下記の非特許文献１には、鍵サーバが、暗号通信に用いられる鍵や設定情報（Security Association）を、予めグループとして登録されている複数の通信端末に配付し、暗号通信を行うそれぞれの通信端末は、当該鍵サーバから配付された鍵等の情報を用いて、グループ内の他の通信端末と暗号通信を行う技術が開示されている。非特許文献１に開示されている技術により、それぞれの通信端末は、暗号通信に用いる鍵等の情報を生成することによって発生する処理負荷を軽減することができる。
【０００３】
【非特許文献１】Internet RFC/STD/FYI/BCP Archives、"RFC 3740 - The Multicast Group Security Architecture"、[平成１８年２月１日検索]、インターネット<URL:http://www.faqs.org/rfcs/rfc3740.html>
【発明の開示】

【発明が解決しようとする課題】
【０００４】
ところで、グループとして登録されている通信端末の数が多くなると、グループ内の通信端末全てが一斉に暗号通信に参加するような使い方の他に、グループとして登録されている通信端末であっても、グループ内の暗号通信に参加している通信端末間のみで、暗号通信を行うような使い方がされる場合がある。つまり、グループ内の暗号通信サービスの提供を受けるためにログインしている通信端末に対してのみにグループ内の暗号通信サービスを提供し、起動していない通信端末や、ネットワークを介して通信可能な状態であるが、グループ内の暗号通信サービスの提供を受けるためにログインしていない通信端末等に対しては、グループ内の暗号通信サービスが提供されないような使い方が想定される。
【０００５】
上記非特許文献１に記載の技術では、グループ内の暗号通信サービスの提供を受けるためにログインするという概念が考慮されておらず、複数の通信端末間で暗号通信を行う場合、鍵サーバで生成された鍵等の情報は、予めグループとして登録されている複数の通信端末の全てに配布される。また、鍵等の情報の配布方法については、上記非特許文献１には特に規定されていないが、予めグループとして登録されている複数の通信端末のそれぞれへ、ユニキャストにより配布することが考えられる。その場合、グループ内の暗号通信サービスの提供を受けるためにログインしていない通信端末に対しても、グループ内の暗号通信に用いられる鍵等の情報が配布され、ネットワークに無駄なトラフィックが発生する場合があった。
【０００６】
また、鍵等の情報の配布を、ブロードキャストやマルチキャストによって行うことにより、鍵等の情報の配布によって発生するトラフィックを低く抑えることも考えられる。しかし、ブロードキャストによって鍵等の情報が配布される場合、鍵サーバが、暗号通信を行うグループに属する通信端末と同一のセグメントに配置される必要がある。そのため、鍵サーバが属するセグメントとは異なるセグメントで実現されているグループに対しては、鍵サーバは、やはりユニキャストにより鍵等の情報を配布する必要があり、無駄なトラフィックが発生する場合がある。
【０００７】
また、マルチキャストによって鍵等の情報が配布される場合、鍵サーバやそれぞれの通信端末の設定のみならず、ネットワーク内のそれぞれの中継装置についてもマルチキャストアドレスの転送に関する設定が行われる必要があり、グループの追加や削除、グループ内の通信端末の追加や削除等の運用管理にかかるコストが膨大となる場合がある。そのため、マルチキャストによって鍵等の情報が配布されることは現実的ではなく、鍵サーバは、やはりユニキャストにより鍵等の情報を配布することになり、無駄なトラフィックが発生する場合がある。
【課題を解決するための手段】
【０００８】
本発明は上記事情に鑑みてなされたものであり、本発明は、グループ内の暗号通信に用いられる鍵や設定情報等を配布することにより発生するトラフィックをより少なくするものである。
【０００９】
すなわち、本発明の暗号通信システムは、グループに所属する複数の通信端末のリストおよび当該複数の通信端末のそれぞれがグループ内の暗号通信に参加している（例えばログインしている）か否かを示す情報をデータベースに保持し、当該暗号通信システムは、当該データベースを参照して、グループに所属しており、かつ、グループ内での暗号通信に参加している通信端末を特定し、特定した通信端末間で用いられる暗号通信用の鍵を生成し、当該特定した通信端末に配付するものである。
【００１０】
例えば、本発明の第１の態様は、セッション管理サーバによって生成された鍵情報を用

いて、複数の通信端末で構成されるグループ内で行われるグループ内暗号通信を実現する暗号通信システムであって、それぞれの通信端末に関する情報を格納するデータベースと、複数の通信端末によって実行されるグループ内暗号通信を管理する端末状態管理サーバとを備え、データベースは、通信端末を識別する端末ＩＤに対応付けて、グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納する参加端末アドレス格納手段と、複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納するグループメンバ情報格納手段とを有し、端末状態管理サーバは、グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づきグループメンバ格納手段を参照して、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出手段と、参加端末アドレス格納手段を参照して、グループメンバ抽出手段によって抽出された端末ＩＤの中から、端末アドレスに対応付けられて参加端末アドレス格納手段内に格納されている端末ＩＤを抽出して、セッション管理サーバへ出力することにより、セッション管理サーバに、グループ内暗号通信要求に含まれるグループＩＤに対応するグループ内の参加端末のそれぞれへ、当該グループ内でのグループ内暗号通信に用いる鍵情報を配布させる参加端末ＩＤ抽出手段とを有することを特徴とする暗号通信システムを提供する。

【００１１】

また、本発明の第２の態様は、複数の通信端末で構成されるグループ内の暗号通信であるグループ内暗号通信を実現する暗号通信システムであって、それぞれの通信端末に関する情報を格納するデータベースと、複数の通信端末によって実行されるグループ内暗号通信を管理する端末状態管理サーバと、グループ内暗号通信に用いられる鍵情報を生成してそれぞれの通信端末へ配布するセッション管理サーバと、複数の通信端末とを備え、データベースは、通信端末を識別する端末ＩＤに対応付けて、グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納する参加端末アドレス格納手段と、複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納するグループメンバ情報格納手段と、参加端末のそれぞれがグループ内暗号通信において実行可能な１つ以上の通信条件を、端末ＩＤに対応付けて格納する通信条件格納手段とを有し、端末状態管理サーバは、セッション管理サーバを介して、グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づいてグループメンバ格納手段を参照して、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出手段と、参加端末アドレス格納手段を参照して、グループメンバ抽出手段によって抽出された端末ＩＤの中から、端末アドレスに対応付けられて参加端末アドレス格納手段内に格納されている端末ＩＤを抽出して、セッション管理サーバへ出力する参加端末ＩＤ抽出手段とを有し、セッション管理サーバは、通信端末との間で暗号通信路を確立し、確立した暗号通信路を介して、当該通信端末とデータを送受信するサーバ側暗号通信手段と、通信端末から、暗号通信路を介して、グループ内暗号通信に参加する旨を通知された場合に、当該通信端末の端末アドレスを参加端末の端末アドレスとして、端末ＩＤに対応付けて参加端末アドレス格納手段に格納する参加端末登録手段と、参加端末ＩＤ抽出手段から出力された端末ＩＤを受信し、受信した端末ＩＤのそれぞれに対応付けられている通信条件を通信条件格納手段から抽出し、抽出した通信条件の中から複数の端末ＩＤに共通の通信条件を抽出し、抽出した通信条件において実行可能なグループ内暗号通信に用いられる鍵情報を生成し、生成した鍵情報を、参加端末ＩＤ抽出手段から受信した端末ＩＤに対応する通信端末のそれぞれへ、暗号通信路を介して送信する鍵生成配布手段とを有し、複数の通信端末のそれぞれは、セッション管理サーバとの間で暗号通信路を確立し、確立した暗号通信路を介して、当該セッション管理サーバとデータを送受信する端末側暗号通信手段と、グループ内暗号通信を開始する場合に、グループ内暗号通信要求を、暗号通信路を介してセッション管理サーバへ送信する暗号通信要求手段と、セッション管理サーバから、グループ内暗号通信要求に応答して、鍵情報を暗号通信路を介して受信した場合に、当該鍵情報を用いてグループ内の他の通信端末との間でグループ内暗号通信を実行するグループ内暗号通信手段とを有する

ことを特徴とする暗号通信システムを提供する。

【００１２】

また、本発明の第３の態様は、セッション管理サーバによって生成された鍵情報を用いて、複数の通信端末で構成されるグループ内で行われるグループ内暗号通信を実現する暗号通信システムにおいて、記憶装置に格納された情報を用いて鍵情報の配布をセッション管理サーバに指示する端末状態管理サーバであって、グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づいて記憶装置を参照し、複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納している、記憶装置内のグループメンバ情報格納手段から、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出手段と、通信端末を識別する端末ＩＤに対応付けて、グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納している、記憶装置内の参加端末アドレス格納手段を参照して、グループメンバ抽出手段によって抽出された端末ＩＤの中から、端末アドレスに対応付けられて参加端末アドレス格納手段内に格納されている端末ＩＤを抽出してセッション管理サーバへ出力することにより、セッション管理サーバに、グループ内暗号通信要求に含まれるグループＩＤに対応するグループ内の参加端末のそれぞれへ、当該グループ内でのグループ内暗号通信に用いる鍵情報を配布させる参加端末ＩＤ抽出手段とを備えることを特徴とする端末状態管理サーバを提供する。

【００１３】

また、本発明の第４の態様は、セッション管理サーバによって生成された鍵情報を用いて、複数の通信端末で構成されるグループ内で行われるグループ内暗号通信を実現する暗号通信システムにおける暗号通信方法であって、暗号通信システムは、それぞれの通信端末に関する情報を格納するデータベースと、複数の通信端末によって実行されるグループ内暗号通信を管理する端末状態管理サーバとを備え、データベースは、通信端末を識別する端末ＩＤに対応付けて、グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納する参加端末アドレス格納手段と、複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納するグループメンバ情報格納手段とを有し、端末状態管理サーバは、グループＩＤを含むグループ内暗号通信要求を受信した場合に、当該グループＩＤに基づいてグループメンバ格納手段を参照して、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出ステップと、参加端末アドレス格納手段を参照して、グループメンバ抽出ステップにおいて抽出した端末ＩＤの中から、端末アドレスに対応付けられて参加端末アドレス格納手段内に格納されている端末ＩＤを抽出してセッション管理サーバへ出力することにより、グループ内暗号通信要求に含まれるグループＩＤに対応するグループ内の参加端末のそれぞれへ、当該グループ内でのグループ内暗号通信に用いる鍵情報を生成して配布させる参加端末ＩＤ抽出ステップとを実行することを特徴とする暗号通信方法を提供する。

【００１４】

また、本発明の第５の態様は、複数の通信端末で構成されるグループ内の暗号通信であるグループ内暗号通信を実現する暗号通信システムにおける暗号通信方法であって、暗号通信システムは、それぞれの通信端末に関する情報を格納するデータベースと、複数の通信端末によって実行されるグループ内暗号通信を管理する端末状態管理サーバと、グループ内暗号通信に用いられる鍵情報を生成してそれぞれの通信端末へ配布するセッション管理サーバと、複数の通信端末とを備え、データベースは、通信端末を識別する端末ＩＤに対応付けて、グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納する参加端末アドレス格納手段と、複数の通信端末のそれぞれの端末ＩＤを、当該通信端末が属するグループを識別するグループＩＤに対応付けて格納するグループメンバ情報格納手段と、参加端末のそれぞれがグループ内暗号通信において実行可能な１つ以上の通信条件を、端末ＩＤに対応付けて格納する通信条件格納手段とを有し、端末状態管理サーバは、セッション管理サーバを介して、グループＩＤを含むグループ内暗

号通信要求を受信した場合に、当該グループＩＤに基づいてグループメンバ格納手段を参照して、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出ステップと、参加端末アドレス格納手段を参照して、グループメンバ抽出ステップにおいて抽出した端末ＩＤの中から、端末アドレスに対応付けられて参加端末アドレス格納手段内に格納されている端末ＩＤを抽出して、セッション管理サーバへ出力する参加端末ＩＤ抽出ステップとを行い、セッション管理サーバは、通信端末との間で暗号通信路を確立し、確立した暗号通信路を介して、当該通信端末とデータを送受信するサーバ側暗号通信ステップと、通信端末から、暗号通信路を介して、グループ内暗号通信に参加する旨を通知された場合に、当該通信端末の端末アドレスを参加端末の端末アドレスとして、端末ＩＤに対応付けて参加端末アドレス格納手段に格納する参加端末登録ステップと、参加端末ＩＤ抽出ステップにおいて出力された端末ＩＤを受信し、受信した端末ＩＤのそれぞれに対応付けられている通信条件を通信条件格納手段から抽出し、抽出した通信条件の中から複数の端末ＩＤに共通の通信条件を抽出し、抽出した通信条件において実行可能なグループ内暗号通信に用いられる鍵情報を生成し、生成した鍵情報を、参加端末ＩＤ抽出ステップにおいて出力された端末ＩＤに対応する通信端末のそれぞれへ、暗号通信路を介して送信する鍵生成配布ステップとを行い、複数の通信端末のそれぞれは、セッション管理サーバとの間で暗号通信路を確立し、確立した暗号通信路を介して、当該セッション管理サーバとデータを送受信する端末側暗号通信ステップと、グループ内暗号通信を開始する場合に、グループ内暗号通信要求を、暗号通信路を介してセッション管理サーバへ送信する暗号通信要求ステップと、セッション管理サーバから、グループ内暗号通信要求に応答して、鍵情報を暗号通信路を介して受信した場合に、当該鍵情報を用いてグループ内の他の通信端末との間でグループ内暗号通信を実行するグループ内暗号通信ステップとを実行することを特徴とする暗号通信方法を提供する。

【００１５】

また、本発明の第６の態様は、セッション管理サーバによって生成された鍵情報を用いて、複数の通信端末で構成されるグループ内で行われるグループ内暗号通信を実現する暗号通信システムにおいて、記憶装置に格納された情報を用いて鍵情報の生成をセッション管理サーバに指示する端末状態管理サーバにおける端末状態管理方法であって、端末状態管理サーバは、グループＩＤを含むグループ内暗号通信要求を受信した場合に、記憶装置内のグループメンバ情報格納手段から、当該グループＩＤに対応するグループに属する通信端末の端末ＩＤを抽出するグループメンバ抽出ステップと、通信端末を識別する端末ＩＤに対応付けて、グループ内暗号通信に参加している通信端末である参加端末のそれぞれの端末アドレスを格納している、記憶装置内の参加端末アドレス格納手段を参照して、グループメンバ抽出ステップにおいて抽出した端末ＩＤの中から、端末アドレスに対応付けられて参加端末アドレス格納手段内に格納されている端末ＩＤを抽出してセッション管理サーバへ出力することにより、セッション管理サーバに、グループ内暗号通信要求に含まれるグループＩＤに対応するグループ内の参加端末のそれぞれへ、グループ内でのグループ内暗号通信に用いる鍵情報を配布させる参加端末ＩＤ抽出ステップとを行うことを特徴とする端末状態管理方法を提供する。

【発明の効果】

【００１６】

本発明の暗号通信システムによれば、グループ内の暗号通信に用いられる鍵や設定情報を配布することにより発生するトラフィックをより少なくすることができる。

【発明を実施するための最良の形態】

【００１７】

以下に、本発明の実施の形態について説明する。

【００１８】

図１は、本発明の一実施形態に係る暗号通信システム１０の構成を示すシステム構成図である。暗号通信システム１０は、データベース２０、端末状態管理サーバ３０、セッション管理サーバ４０、および複数の通信端末５０を備える。データベース２０、端末状態

管理サーバ３０、およびセッション管理サーバ４０のそれぞれは、管理ネットワーク１１に接続されており、管理ネットワーク１１を介して互いに通信する。セッション管理サーバ４０は、さらにユーザネットワーク１２に接続されている。

【００１９】

複数の通信端末５０のそれぞれは、例えば汎用コンピュータ、携帯情報端末、ＩＰ（Internet Protocol）電話器、または通信機能を有するサーバ等であり、インターネット等のユーザネットワーク１２に接続され、ユーザネットワーク１２を介してセッション管理サーバ４０や他の通信端末５０と通信する。ここで、複数の通信端末５０は、２つ以上の通信端末５０毎にグループを構成しており、それぞれの通信端末５０は、セッション管理サーバ４０から配布される鍵情報を用いて、グループ内の１つ以上の他の通信端末５０とグループ内暗号通信を行う。

【００２０】

データベース２０は、それぞれの通信端末５０の通信条件、ログイン中の通信端末５０の識別情報、およびそれぞれのグループに属する通信端末５０の識別情報等を格納している。端末状態管理サーバ３０は、グループ内暗号通信を行うグループを識別するグループＩＤを含む通信開始要求をセッション管理サーバ４０を介して通信端末５０から受信した場合に、データベース２０を参照して、当該グループＩＤに対応するグループに属する通信端末５０であって、ログイン中の通信端末５０の識別情報を抽出する。そして、端末状態管理サーバ３０は、グループ内暗号通信に使用される鍵情報の生成指示を、抽出した識別情報と共にセッション管理サーバ４０へ送信する。

【００２１】

セッション管理サーバ４０は、通信端末５０の識別情報である端末ＩＤおよび端末アドレスを含む暗号通信路確立要求をそれぞれの通信端末５０から受け付けることによりログイン処理を開始し、ログインに関する認証等に成功した場合に、当該暗号通信路確立要求に含まれる端末アドレスを端末状態管理サーバ３０に登録する。また、セッション管理サーバ４０は、端末ＩＤおよび端末アドレスを含む暗号通信路削除要求をそれぞれの通信端末５０から受け付けた場合に、対応する端末アドレスをデータベース２０から削除する。

【００２２】

また、セッション管理サーバ４０は、端末ＩＤと共に鍵情報の生成指示を端末状態管理サーバ３０から受信した場合に、データベース２０を参照して、受信した端末ＩＤに対応する通信端末５０の通信条件を抽出する。そして、セッション管理サーバ４０は、抽出した通信条件に基づいて鍵情報を生成し、生成した鍵情報を、当該鍵情報を使用するそれぞれの通信端末５０へ送信する。ここで、鍵情報とは、暗号鍵または当該暗号鍵を生成するための基となる情報であるシードのいずれか、ならびに、当該暗号鍵の鍵長および当該暗号鍵を用いて暗号化するための暗号アルゴリズムの種類等を含む。なお、本実施形態において、暗号鍵またはシードから生成される暗号鍵は、共通鍵暗号方式に基づく暗号通信に使用されるものである。

【００２３】

このように、暗号通信システム１０は、複数の通信端末５０によってグループ内暗号通信が行われる場合に、グループ内暗号通信で使用される鍵情報を、グループに属する通信端末５０であって、ログイン中の通信端末５０のそれぞれへ配布する。従って、暗号通信システム１０は、ユーザネットワーク１２を介して通信可能な状態ではあるが、グループ内の暗号通信サービスの提供を受けるつもりがなく、セッション管理サーバ４０にログインしていない通信端末５０に対して鍵情報を配布しない。そのため、暗号通信システム１０は、鍵情報の配布によって発生するトラフィックをより少なくすることができる。

【００２４】

なお、図１において、管理ネットワーク１１とユーザネットワーク１２とは物理的に異なるネットワークとして描かれているが、管理ネットワーク１１とユーザネットワーク１２とは、ＶＬＡＮ（Virtual LAN）等により物理的に同一のネットワークを論理的に分けることによって構築されていてもよい。また、管理ネットワーク１１には、ユーザネット

ワーク１２よりも高いセキュリティが確保されていることが好ましい。

【００２５】

以下、上記機能を実現するために暗号通信システム１０が有する構成についてさらに詳しく説明する。

【００２６】

図２は、データベース２０の詳細な機能構成の一例を示すブロック図である。データベース２０は、端末アドレス格納部２１、通信条件格納部２２、グループメンバ情報格納部２３、グループアドレス格納部２４、ネットワークＩＦ部２５、およびデータベース制御部２６を備える。

【００２７】

端末アドレス格納部２１は、例えば図３に示すように、通信端末５０の端末ＩＤ２１０に対応付けて、ログイン中の通信端末５０の端末アドレス２１１を格納する。本実施形態において、端末ＩＤ２１０は、例えばＵＲＩ（Uniform Resource Identifier）であり、端末アドレス２１１は、例えばＩＰアドレスである。

【００２８】

通信条件格納部２２は、例えば図４に示すように、それぞれの通信端末５０の端末ＩＤ２２０に対応付けて、当該通信端末５０がグループ内暗号通信において実行可能な通信条件を１つ以上格納する。それぞれの通信条件には、優先順位２２４毎に、対応する通信端末５０によって実行可能な暗号アルゴリズム２２１、暗号通信に用いられる暗号鍵の鍵長２２２、および暗号鍵のハッシュ関数種別２２３等が含まれる。

【００２９】

ここで、暗号アルゴリズム２２１とは、例えば、置換、転字、換字、分割、またはシフト演算等の各種変換処理の順番等といった暗復号化処理（例えば暗復号化プログラム）を特定する情報である。暗号アルゴリズムの代表的なものとしては、ＡＥＳ（Advanced Encryption Standard）等がある。

【００３０】

端末状態管理サーバ３０は、セッション管理サーバ４０を介して、通信端末５０から、当該通信端末５０の端末ＩＤ、端末アドレス、および通信条件を含む通信条件登録要求を受け付けた場合に、当該通信条件登録要求に含まれる端末ＩＤおよび通信条件を通信条件格納部２２に登録する。また、端末状態管理サーバ３０は、セッション管理サーバ４０を介して、通信端末５０から、当該通信端末５０の端末ＩＤを含む通信条件削除要求を受け付けた場合に、当該通信条件削除要求に含まれる端末ＩＤおよび当該端末ＩＤに対応する通信条件を通信条件格納部２２から削除する。

【００３１】

グループメンバ情報格納部２３は、例えば図５に示すように、それぞれのグループに属する通信端末５０の端末ＩＤ２３１を、当該グループを識別するグループＩＤ２３０に対応付けて格納する。

【００３２】

グループアドレス格納部２４は、マルチキャストやブロードキャスト等によってグループ内暗号通信が行なわれるグループについて、例えば図６に示すように、マルチキャストアドレスやブロードキャストアドレス等のグループアドレス２４１を、グループを識別するグループＩＤ２４０に対応付けて格納する。グループ内暗号通信がユニキャストで行われるグループについては、当該グループに対応するグループＩＤは、グループアドレス格納部２４内に格納されない。なお、グループメンバ情報格納部２３およびグループアドレス格納部２４内に格納されるデータは、システム管理者等によって予め設定される。

【００３３】

データベース制御部２６は、ネットワークＩＦ部２５を介して端末状態管理サーバ３０またはセッション管理サーバ４０から受信した各種要求に応じて、端末アドレス格納部２１、通信条件格納部２２、グループメンバ情報格納部２３、およびグループアドレス格納部２４から必要なデータを抽出して返信したり、当該要求に応じて、端末アドレス格納部

２１および通信条件格納部２２内のデータを書き換えたりする処理を行う。

【００３４】

図７は、セッション管理サーバ４０の詳細な機能構成の一例を示すブロック図である。セッション管理サーバ４０は、ネットワークＩＦ部４００、通信条件削除要求転送部４０１、鍵情報生成部４０２、端末アドレス削除部４０３、端末アドレス登録部４０４、通信条件登録要求転送部４０５、通信要求転送部４０６、鍵情報削除要求送信部４０７、暗号通信部４０８、端末認証部４０９、ネットワークＩＦ部４１０、鍵生成部４１１、および所有鍵格納部４１２を備える。

【００３５】

ネットワークＩＦ部４１０は、ユーザネットワーク１２を介して、それぞれの通信端末５０と通信する。ネットワークＩＦ部４００は、管理ネットワーク１１を介して、データベース２０または端末状態管理サーバ３０と通信する。所有鍵格納部４１２は、セッション管理サーバ４０の秘密鍵と、通信端末５０がセッション管理サーバ４０を認証するための、当該秘密鍵と対の公開鍵が真正であることを証明する公開鍵証明書とを格納する。鍵生成部４１１は、暗号通信部４０８が通信端末５０と暗号通信に利用する暗号鍵を生成する。

【００３６】

端末認証部４０９は、ネットワークＩＦ部４１０を介して通信端末５０から暗号通信路確立要求を受信した場合に、当該通信端末５０との間で認証処理を行う。そして、認証が成立した場合に、端末認証部４０９は、鍵生成部４１１に暗号鍵を生成させると共に、所有鍵格納部４１２に格納されているセッション管理サーバ４０の秘密鍵を用いてディジタル署名を生成する。

【００３７】

そして、端末認証部４０９は、生成した暗号鍵、および、ディジタル署名とセッション管理サーバ４０の公開鍵証明書とを含む応答を当該通信端末５０へ送信することにより、当該通信端末５０との間で暗号鍵を共有する。そして、端末認証部４０９は、当該通信端末５０に対応する暗号鍵を暗号通信部４０８に設定する。セッション管理サーバ４０と当該通信端末５０との間の通信は、共有された暗号鍵を用いて行われる。

【００３８】

ここで、本実施形態において、通信端末５０によるログインとは、セッション管理サーバ４０と当該通信端末５０との間で暗号鍵が共有された後に、セッション管理サーバ４０が、当該通信端末５０から送信された通信条件登録要求６０に基づいて、データベース２０の端末アドレス格納部２１に当該通信端末５０の端末アドレスを登録すると共に、端末状態管理サーバ３０を介して、通信条件格納部２２に当該通信端末５０の通信条件を登録することを指す。また、ログイン中の通信端末５０とは、セッション管理サーバ４０との間で有効な暗号鍵が共有されており、かつ、端末アドレス格納部２１に端末アドレスが登録されており、かつ、通信条件格納部２２に通信条件が登録されている通信端末５０を指す。また、通信端末５０によるログアウトとは、セッション管理サーバ４０が、データベース２０の端末アドレス格納部２１から当該通信端末５０の端末アドレスを削除すると共に、端末状態管理サーバ３０を介して、通信条件格納部２２から当該通信端末５０の通信条件を削除した後に、セッション管理サーバ４０と当該通信端末５０との間で共有されている有効な暗号鍵が両装置において破棄されることを指す。

【００３９】

端末アドレス登録部４０４および通信条件登録要求転送部４０５は、暗号通信部４０８を介して、グループ内暗号通信に参加する旨を示す情報である通信条件登録要求を通信端末５０から受信する。通信条件登録要求６０は、例えば図８に示すようなデータ構造を有する。通信条件登録要求６０には、通信条件登録要求であることを示すメッセージ種別６００、当該通信条件登録要求６０の送信元の通信端末５０の端末アドレス６０１、当該通信端末５０の端末ＩＤ６０２、および当該通信端末５０が実現可能な１つ以上の通信条件６０３が含まれる。それぞれの通信条件６０３には、暗号アルゴリズム６０５、鍵長６０

６、ハッシュ関数種別６０７、および優先順位６０８等が含まれる。

【００４０】

端末アドレス登録部４０４は、受信した通信条件登録要求６０内の端末アドレス６０１を、ネットワークＩＦ部４００を介して、データベース２０の端末アドレス格納部２１へ送り、登録完了を示す応答を受信した場合に、その旨を通信条件登録要求転送部４０５に通知する。端末アドレス登録部４０４から登録完了の通知を受けた場合に、通信条件登録要求転送部４０５は、通信条件登録要求６０を、ネットワークＩＦ部４００を介して、端末状態管理サーバ３０へ転送する。そして、端末状態管理サーバ３０から登録完了通知を受信した場合に、通信条件登録要求転送部４０５は、受信した登録完了通知を暗号通信部４０８を介して、当該通信条件登録要求６０を送信してきた通信端末５０へ送信する。

【００４１】

通信要求転送部４０６は、暗号通信部４０８を介して、通信開始要求または通信終了要求を通信端末５０から受信し、受信した通信開始要求または通信終了要求を、ネットワークＩＦ部４００を介して端末状態管理サーバ３０へ転送する。また、通信要求転送部４０６は、ネットワークＩＦ部４００を介して、通信開始拒否応答または通信終了拒否応答を端末状態管理サーバ３０から受信した場合に、受信した通信開始拒否応答または通信終了拒否応答を、暗号通信部４０８を介して通信端末５０へ転送する。

【００４２】

鍵情報生成部４０２は、ネットワークＩＦ部４００を介して、グループ内暗号通信に用いられる鍵情報の生成指示を端末状態管理サーバ３０から受信する。鍵情報生成指示６１は、例えば図９に示すようなデータ構造を有する。鍵情報生成指示６１には、鍵情報生成指示を示すメッセージ種別６１０、生成すべき鍵情報の有効期限６１１、暗号通信が行われるグループのグループＩＤ６１２、および端末ＩＤ一覧６１３が含まれる。端末ＩＤ一覧６１３には、グループＩＤ６１２に対応するグループに属する１つ以上の通信端末５０であって、現在ログイン中の通信端末５０の端末ＩＤ６１３０が含まれる。

【００４３】

鍵情報生成部４０２は、端末ＩＤ６１３０を含む通信条件取得要求を、ネットワークＩＦ部４００を介して、データベース２０へ送信することにより、当該端末ＩＤ６１３０に対応するそれぞれの通信端末５０の通信条件を取得する。そして、鍵情報生成部４０２は、取得したそれぞれの通信端末５０の通信条件に基づいて、それぞれの通信端末５０に共通の通信条件を抽出する。そして、鍵情報生成部４０２は、抽出した通信条件において実行可能なグループ内暗号通信で用いられる鍵を含む鍵情報を生成する。

【００４４】

そして、鍵情報生成部４０２は、鍵情報生成指示６１に含まれるグループＩＤ６１２に基づいて、ネットワークＩＦ部４００を介して、データベース２０のグループアドレス格納部２４を参照し、当該グループＩＤ６１２に対応するグループアドレス２４１が存在する場合には、当該グループＩＤ６１２に対応するグループアドレス２４１を取得する。また、鍵情報生成部４０２は、鍵情報生成指示６１に含まれる端末ＩＤ６１３０に基づいて、ネットワークＩＦ部４００を介して、データベース２０の端末アドレス格納部２１を参照して、それぞれの端末ＩＤ６１３０に対応する端末アドレス２１１を取得する。

【００４５】

そして、鍵情報生成部４０２は、生成した鍵情報等に基づいて、例えば図１０に示すような配布鍵情報６２を生成する。配布鍵情報６２には、配布鍵情報であることを示すメッセージ種別６２０、鍵情報６２１、端末アドレス一覧６２２、端末ＩＤ一覧６２３、およびグループアドレス６２４が含まれる。

【００４６】

鍵情報６２１には、鍵情報６２１の有効期限６２１０、暗号アルゴリズム６２１１、鍵長６２１２、暗号鍵６２１３、およびハッシュ関数種別６２１４等が含まれる。なお、鍵情報６２１内には、暗号鍵６２１３に代えて、シードが含まれていてもよい。端末アドレス一覧６２２には、暗号通信を行うグループに属する１つ以上の通信端末５０であって、

ログイン中の通信端末５０の端末アドレス６２２０が含まれる。端末ＩＤ一覧６２３には、暗号通信を行うグループに属する通信端末５０であって、ログイン中の通信端末５０の端末ＩＤ６２３０が含まれる。なお、グループに対応するグループアドレスがデータベース２０のグループアドレス格納部２４に格納されていない場合には、グループアドレス６２４にはｎｕｌｌデータが含まれる。

【００４７】

鍵情報生成部４０２は、生成した配布鍵情報６２を、当該配布鍵情報６２内の端末アドレス６２２０のそれぞれに対応する通信端末５０へ、暗号通信部４０８を介して、例えばユニキャストにより送信する。このように、セッション管理サーバ４０は、生成した鍵情報と共に、当該鍵情報を用いてグループ内暗号通信を行う通信端末５０の端末ＩＤおよび端末アドレスを配布するので、それぞれの通信端末５０は、グループ内暗号通信に参加している他の通信端末５０の存在を認識することができる。

【００４８】

また、鍵情報生成部４０２は、ネットワークＩＦ部４００を介して、グループ内暗号通信に用いられている鍵情報の再配布指示を端末状態管理サーバ３０から受信する。鍵情報再配布指示は、メッセージ種別６１０が鍵情報生成指示６１とは異なるのみで、それ以外は図９に示した鍵情報生成指示６１と同様のデータ構造を有する。鍵情報再配布指示を受信した場合、鍵情報生成部４０２は、鍵情報生成指示６１を受信した場合と同様に、当該鍵情報再配布指示に含まれる情報に基づいて図１０に示した配布鍵情報６２を生成し、生成した配布鍵情報６２を対応する通信端末５０に配布する。

【００４９】

鍵情報削除要求送信部４０７は、ネットワークＩＦ部４００を介して、端末状態管理サーバ３０から、端末ＩＤを含む鍵情報削除要求を受信した場合に、当該鍵情報削除要求に含まれる端末ＩＤで特定される端末５０へ、受信した鍵情報削除要求を、暗号通信部４０８を介して送信する。

【００５０】

通信条件削除要求転送部４０１および端末アドレス削除部４０３は、暗号通信部４０８を介して、通信端末５０から、グループ内暗号通信への参加をやめる旨を示す情報である通信条件削除要求を受信する。当該通信条件削除要求には、当該通信端末５０の端末ＩＤが含まれる。通信条件削除要求転送部４０１は、受信した通信条件削除要求を、ネットワークＩＦ部４００を介して端末状態管理サーバ３０へ転送する。そして、ネットワークＩＦ部４００を介して端末状態管理サーバ３０から削除完了通知を受信した場合に、通信条件削除要求転送部４０１は、その旨を端末アドレス削除部４０３に通知する。

【００５１】

通信条件削除要求転送部４０１から削除完了を通知された場合に、端末アドレス削除部４０３は、通信条件削除要求に含まれる端末ＩＤに対応する端末アドレスを、データベース２０の端末アドレス格納部２１から削除し、削除完了通知を、暗号通信部４０８を介して、通信条件削除要求を送信してきた通信端末５０へ送信する。

【００５２】

図１１は、端末状態管理サーバ３０の詳細な機能構成の一例を示すブロック図である。端末状態管理サーバ３０は、鍵情報生成指示格納部３００、鍵情報生成指示部３０１、鍵情報削除指示部３０２、通信条件登録部３０３、通信条件削除部３０４、グループメンバ判定部３０５、およびネットワークＩＦ部３０６を備える。

【００５３】

ネットワークＩＦ部３０６は、管理ネットワーク１１を介して、データベース２０またはセッション管理サーバ４０と通信する。通信条件登録部３０３は、ネットワークＩＦ部３０６を介して、セッション管理サーバ４０から、図８に示した通信条件登録要求６０を受信した場合に、受信した通信条件登録要求６０に含まれる通信条件および端末ＩＤをデータベース２０へ送信することにより、当該通信条件を当該端末ＩＤに対応付けて通信条件格納部２２に登録させる。そして、通信条件登録部３０３は、データベース２０から登

録完了を示す応答を受信した場合に、登録完了通知を、ネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信する。

【００５４】

通信条件削除部３０４は、ネットワークＩＦ部３０６を介して、セッション管理サーバ４０から、端末ＩＤを含む通信条件削除要求を受信した場合に、当該端末ＩＤをデータベース２０へ送信することにより、当該端末ＩＤおよび当該端末ＩＤに対応付けて登録されている通信条件を通信条件格納部２２から削除させる。そして、通信条件削除部３０４は、データベース２０から削除完了を示す応答を受信した場合に、削除完了通知を、ネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信する。

【００５５】

グループメンバ判定部３０５は、ネットワークＩＦ部３０６を介して、セッション管理サーバ４０から、送信元の通信端末５０の端末ＩＤおよび暗号通信を行うグループのグループＩＤを含む通信開始要求を受信した場合に、当該グループＩＤを含むグループメンバ取得要求をデータベース２０へ送信することにより、当該グループＩＤに対応付けられてグループメンバ情報格納部２３に格納されている端末ＩＤをデータベース２０から取得する。そして、グループメンバ判定部３０５は、取得した端末ＩＤに基づいて、当該通信開始要求に含まれる端末ＩＤが、取得した端末ＩＤに含まれているか否かを判定する。

【００５６】

当該通信開始要求に含まれる端末ＩＤが、データベース２０から取得した端末ＩＤに含まれていない場合、グループメンバ判定部３０５は、当該端末ＩＤを含む通信開始拒否応答をネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信する。

【００５７】

当該通信開始要求に含まれる端末ＩＤが、データベース２０から取得した端末ＩＤに含まれている場合、グループメンバ判定部３０５は、当該通信開始要求に含まれるグループＩＤおよびデータベース２０から取得した端末ＩＤを鍵情報生成指示部３０１へ送信する。

【００５８】

また、グループメンバ判定部３０５は、ネットワークＩＦ部３０６を介して、セッション管理サーバ４０から、送信元の通信端末５０の端末ＩＤおよび暗号通信を行っているグループのグループＩＤを含む通信終了要求を受信した場合に、当該グループＩＤを含むグループメンバ取得要求をデータベース２０へ送信することにより、当該グループＩＤに対応付けられてグループメンバ情報格納部２３に格納されている端末ＩＤを取得する。そして、グループメンバ判定部３０５は、取得した端末ＩＤに基づいて、当該通信終了要求に含まれる端末ＩＤが、取得した端末ＩＤに含まれているか否かを判定する。

【００５９】

当該通信終了要求に含まれる端末ＩＤが、データベース２０から取得した端末ＩＤに含まれていない場合、グループメンバ判定部３０５は、当該端末ＩＤを含む通信終了拒否応答をネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信する。

【００６０】

当該通信終了要求に含まれる端末ＩＤが、データベース２０から取得した端末ＩＤに含まれている場合、グループメンバ判定部３０５は、当該通信終了要求に含まれるグループＩＤおよびデータベース２０から取得した端末ＩＤを鍵情報削除指示部３０２へ送信する。

【００６１】

鍵情報生成指示部３０１は、グループメンバ判定部３０５からグループＩＤおよび端末ＩＤを受信した場合に、グループメンバ判定部３０５から受信した端末ＩＤを含むログイン中端末ＩＤ取得要求をデータベース２０へ送信することにより、当該端末ＩＤの中で、端末アドレス格納部２１内に端末アドレスが対応付けられているものを取得する。これにより、鍵情報生成指示部３０１は、当該グループＩＤに対応するグループに属する通信端末５０の中で、現在ログイン中の通信端末５０の端末ＩＤを抽出することができる。また

、鍵情報生成指示部３０１は、生成すべき鍵情報の有効期限を設定する。

【００６２】

そして、鍵情報生成指示部３０１は、図９に示したように、設定した有効期限６１１、鍵情報生成指示格納部３００から受信したグループＩＤ６１２、および抽出した端末ＩＤ一覧６１３を含む鍵情報生成指示６１を生成し、生成した鍵情報生成指示６１を、ネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信する。そして、鍵情報生成指示部３０１は、送信した鍵情報生成指示６１を鍵情報生成指示格納部３００に格納する。鍵情報生成指示格納部３００には、例えば図１２に示すように、鍵情報生成指示６１に含まれるグループＩＤ３００１および端末ＩＤ一覧３００２が、有効期限３０００に対応付けられて格納される。

【００６３】

また、鍵情報生成指示部３０１は、所定のタイミングで鍵情報生成指示格納部３００を参照し、有効期限の経過前であって、現在時刻との差が所定値以下となる有効期限３０００が存在するか否かを判定する。現在時刻との差が所定値以下となる有効期限３０００が存在する場合、鍵情報生成指示部３０１は、当該有効期限３０００に対応するグループＩＤ３００１および端末ＩＤ一覧３００２を鍵情報生成指示格納部３００から抽出し、当該有効期限３０００、グループＩＤ３００１、端末ＩＤ一覧３００２を鍵情報生成指示格納部３００から削除する。

【００６４】

そして、鍵情報生成指示部３０１は、新たに有効期限を設定し、設定した有効期限と、鍵情報生成指示格納部３００から抽出したグループＩＤ３００１および端末ＩＤ一覧３００２とを含む鍵情報再生成指示を生成し、生成した鍵情報再生成指示をネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信する。そして、鍵情報生成指示部３０１は、送信した鍵情報再生成指示を鍵情報生成指示格納部３００に格納する。なお、鍵情報再生成指示は、図９に示した鍵情報生成指示６１においてメッセージ種別６１０が異なるのみで鍵情報生成指示６１と略同様のデータ構造である。

【００６５】

鍵情報削除指示部３０２は、グループメンバ判定部３０５からグループＩＤおよび端末ＩＤを受信した場合に、当該端末ＩＤを含むログイン中端末ＩＤ取得要求をデータベース２０へ送信することにより、当該端末ＩＤの中で、端末アドレス格納部２１内に端末アドレスが対応付けられているものを取得する。

【００６６】

そして、鍵情報削除指示部３０２は、データベース２０から取得した端末ＩＤを含む鍵情報削除要求を生成し、生成した鍵情報削除要求を、ネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信する。そして、鍵情報削除指示部３０２は、グループメンバ判定部３０５から受信したグループＩＤ、当該グループＩＤに対応付けて格納されている有効期限、および端末ＩＤ一覧を、鍵情報生成指示格納部３００から削除する。

【００６７】

図１３は、通信端末５０の詳細な機能構成の一例を示すブロック図である。通信端末５０は、ネットワークＩＦ部５００、端末用暗号通信部５０１、鍵情報取得部５０２、サーバ用暗号通信部５０３、所有鍵格納部５０４、鍵情報格納部５０５、通信終了要求部５０６、通信条件削除要求部５０７、通信開始要求部５０８、通信条件登録要求部５０９、アプリケーション部５１０、および通信条件格納部５１１を備える。

【００６８】

所有鍵格納部５０４は、自通信端末５０の秘密鍵と、セッション管理サーバ４０が自通信端末を認証するための、当該秘密鍵と対の公開鍵証明書とを格納している。サーバ用暗号通信部５０３は、アプリケーション部５１０からの指示を受けて、ネットワークＩＦ部５００を介して、所有鍵格納部５０４内の秘密鍵および公開鍵証明書を用いて、セッション管理サーバ４０との間で暗号鍵の共有処理を行う。その後、サーバ用暗号通信部５０３は、セッション管理サーバ４０と共有した暗号鍵を用いてセッション管理サーバ４０と通

信する。

【００６９】

また、サーバ用暗号通信部５０３は、アプリケーション部５１０からの指示を受けて、ネットワークＩＦ部５００を介してセッション管理サーバ４０へ暗号通信路削除要求を送信することにより、セッション管理サーバ４０との間で共有している暗号鍵を破棄する。

【００７０】

通信条件格納部５１１は、例えば図１４に示すようなデータ構造を有し、１つ以上の通信条件のそれぞれを、優先順位５１１３に対応付けて格納している。それぞれの通信条件には、自通信端末５０によって実行可能な暗号アルゴリズム５１１０、暗号通信に用いられる暗号鍵の鍵長５１１１、およびハッシュ関数種別５１１２等が含まれる。

【００７１】

通信条件登録要求部５０９は、アプリケーション部５１０からの指示に従い、通信条件格納部５１１を参照して、図８に示した通信条件登録要求６０を生成し、生成した通信条件登録要求６０を、サーバ用暗号通信部５０３を介してセッション管理サーバ４０へ送信する。

【００７２】

通信条件削除要求部５０７は、アプリケーション部５１０からの指示に従い、自通信端末５０の端末ＩＤを含む通信条件削除要求を、サーバ用暗号通信部５０３を介してセッション管理サーバ４０へ送信する。

【００７３】

通信開始要求部５０８は、アプリケーション部５１０からの指示に従い、自通信端末５０の端末ＩＤおよび暗号通信を行うグループのグループＩＤを含む通信開始要求を、サーバ用暗号通信部５０３を介してセッション管理サーバ４０へ送信する。

【００７４】

通信終了要求部５０６は、アプリケーション部５１０からの指示に従い、自通信端末５０の端末ＩＤおよび暗号通信を行うグループのグループＩＤを含む通信終了要求を、サーバ用暗号通信部５０３を介してセッション管理サーバ４０へ送信する。

【００７５】

鍵情報取得部５０２は、サーバ用暗号通信部５０３を介して、図１０に示した配布鍵情報６２を受信した場合に、受信した配布鍵情報６２に含まれる鍵情報６２１、端末アドレス一覧６２２、および端末ＩＤ一覧６２３を鍵情報格納部５０５に格納する。通信端末５０にインストールされているグループ内ネットワーク通信を行うアプリケーションが通信パケットを送受信する際に、端末用暗号通信部５０１は、鍵情報格納部５０５を検索して、そのパケットの通信先が図１０の配付鍵情報６２の端末アドレス６２２０あるいは、グループアドレス６２４に含まれているかどうか判定し、含まれていた場合には、鍵情報６２１を用いて、他の通信端末５０との間でグループ内暗号通信を行う。

【００７６】

また、鍵情報格納部５０５内に既に鍵情報６２１、端末アドレス一覧６２２、および端末ＩＤ一覧６２３が格納されている場合には、鍵情報取得部５０２は、新たに配布鍵情報６２を受信すると、その配布鍵情報６２の鍵情報６２１、端末アドレス一覧６２２、および端末ＩＤ一覧６２３で、鍵情報格納部５０５内のデータを更新する。

【００７７】

また、鍵情報取得部５０２は、サーバ用暗号通信部５０３を介して、鍵情報削除要求を受信した場合に、鍵情報格納部５０５に格納されている鍵情報６２１、端末アドレス一覧６２２、および端末ＩＤ一覧６２３を鍵情報格納部５０５から削除する。

【００７８】

アプリケーション部５１０は、グループに属する通信端末５０であって、現在ログイン中の通信端末５０の端末ＩＤおよび端末アドレスの情報を、鍵情報格納部５０５から得ることができる。これにより、通信端末５０は、現在行われているグループ内暗号通信に、グループ内の他の通信端末５０のいずれが参加しているかを認識することができる。

【００７９】
図１５は、データベース２０、端末状態管理サーバ３０、またはセッション管理サーバ４０の機能を実現する情報処理装置７０のハードウェア構成の一例を示すハードウェア構成図である。情報処理装置７０は、ＣＰＵ（Central Processing Unit）７１、ＲＡＭ（Random Access Memory）７２、ＲＯＭ（Read Only Memory）７３、ＨＤＤ（Hard Disk Drive）７４、通信インターフェイス７５、入出力インターフェイス７６、メディアインターフェイス７７を備える。
【００８０】
ＣＰＵ７１は、ＲＯＭ７３およびＨＤＤ７４に格納されたプログラムに基づいて動作し、各部の制御を行う。ＲＯＭ７３は、情報処理装置７０の起動時にＣＰＵ７１が実行するブートプログラムや、情報処理装置７０のハードウェアに依存するプログラム等を格納する。
【００８１】
ＨＤＤ７４は、ＣＰＵ７１が実行するプログラムおよびＣＰＵ７１が使用するデータ等を格納する。通信インターフェイス７５は、管理ネットワーク１１またはユーザネットワーク１２を介して他の機器からデータを受信してＣＰＵ７１へ送ると共に、ＣＰＵ７１が生成したデータを、これらのネットワークを介して他の機器へ送信する。
【００８２】
ＣＰＵ７１は、入出力インターフェイス７６を介して、キーボードやマウス、ＬＣＤ（Liquid Crystal Display）等の入出力装置を制御する。ＣＰＵ７１は、入出力インターフェイス７６を介して、キーボードやマウス等からデータを取得する。また、ＣＰＵ７１は、生成したデータを、入出力インターフェイス７６を介してＬＣＤ等へ出力する。
【００８３】
メディアインターフェイス７７は、記録媒体７８に格納されたプログラムまたはデータを読み取り、ＲＡＭ７２に提供する。ＲＡＭ７２を介してＣＰＵ７１に提供されるプログラムは、記録媒体７８に格納されている。当該プログラムは、記録媒体７８から読み出されて、ＲＡＭ７２を介して情報処理装置７０にインストールされ、ＣＰＵ７１によって実行される。
【００８４】
情報処理装置７０がデータベース２０として機能する場合、ＨＤＤ７４には、端末アドレス格納部２１、通信条件格納部２２、グループメンバ情報格納部２３、およびグループアドレス格納部２４内のデータが格納され、情報処理装置７０にインストールされて実行されるプログラムは、情報処理装置７０を、ネットワークＩＦ部２５およびデータベース制御部２６として機能させる。
【００８５】
また、情報処理装置７０が端末状態管理サーバ３０として機能する場合、ＨＤＤ７４には鍵情報生成指示格納部３００内のデータが格納され、情報処理装置７０にインストールされて実行されるプログラムは、情報処理装置７０を、鍵情報生成指示部３０１、鍵情報削除指示部３０２、通信条件登録部３０３、通信条件削除部３０４、グループメンバ判定部３０５、およびネットワークＩＦ部３０６としてそれぞれ機能させる。
【００８６】
また、情報処理装置７０がセッション管理サーバ４０として機能する場合、ＨＤＤ７４には所有鍵格納部４１２内のデータが格納され、情報処理装置７０にインストールされて実行されるプログラムは、情報処理装置７０を、ネットワークＩＦ部４００、通信条件削除要求転送部４０１、鍵情報生成部４０２、端末アドレス削除部４０３、端末アドレス登録部４０４、通信条件登録要求転送部４０５、通信要求転送部４０６、鍵情報削除要求送信部４０７、暗号通信部４０８、端末認証部４０９、ネットワークＩＦ部４１０、および鍵生成部４１１としてそれぞれ機能させる。
【００８７】
記録媒体７８は、例えばＤＶＤ、ＰＤ等の光学記録媒体、ＭＯ等の光磁気記録媒体、テ

ープ媒体、磁気記録媒体、または半導体メモリ等である。情報処理装置７０は、これらのプログラムを、記録媒体７８から読み取って実行するが、他の例として、他の装置から、通信媒体を介して、これらのプログラムを取得してもよい。通信媒体とは、管理ネットワーク１１またはユーザネットワーク１２、またはこれらを伝搬するディジタル信号または搬送波を指す。

【００８８】

ここで、グループ内暗号通信を実現する場合の端末状態管理サーバ３０の動作の一例について、図１６を用いて詳細に説明する。例えば電源を投入される等の所定のタイミングで、端末状態管理サーバ３０は、本フローチャートに示す動作を開始する。

【００８９】

まず、通信条件登録部３０３は、管理ネットワーク１１を介して、セッション管理サーバ４０から、図８に示した通信条件登録要求６０を受信したか否かを判定する（Ｓ１００）。通信条件登録要求６０を受信した場合（Ｓ１００：Ｙｅｓ）、通信条件登録部３０３は、受信した通信条件登録要求６０に含まれる通信条件および端末ＩＤをデータベース２０へ送信することにより、当該通信条件を当該端末ＩＤに対応付けて通信条件格納部２２に格納させる（Ｓ１０１）。

【００９０】

そして、通信条件登録部３０３は、データベース２０から登録完了を示す応答を受信し、当該通信条件登録要求６０の送信元の通信端末５０の端末ＩＤを含む登録完了通知を、管理ネットワーク１１を介してセッション管理サーバ４０へ送信し（Ｓ１０２）、通信条件登録部３０３は、再びステップ１００に示した処理を実行する。

【００９１】

通信条件登録要求６０を受信していない場合（Ｓ１００：Ｎｏ）、グループメンバ判定部３０５は、管理ネットワーク１１を介して、通信開始要求を受信したか否かを判定する（Ｓ１０３）。通信開始要求を受信した場合（Ｓ１０３：Ｙｅｓ）、グループメンバ判定部３０５は、当該グループＩＤを含むグループメンバ取得要求をデータベース２０へ送信することにより、当該グループＩＤに対応付けられてグループメンバ情報格納部２３に格納されている端末ＩＤをデータベース２０から取得する。そして、グループメンバ判定部３０５は、取得した端末ＩＤに基づいて、当該通信開始要求に含まれる端末ＩＤが、取得した端末ＩＤに含まれているか否かを判定する（Ｓ１０４）。

【００９２】

当該通信開始要求に含まれる端末ＩＤが、データベース２０から取得した端末ＩＤに含まれている場合（Ｓ１０４：Ｙｅｓ）、グループメンバ判定部３０５は、当該通信開始要求に含まれるグループＩＤおよびデータベース２０から取得した端末ＩＤを鍵情報生成指示部３０１へ送信する。

【００９３】

次に、鍵情報生成指示部３０１は、当該端末ＩＤを含むログイン中端末ＩＤ取得要求をデータベース２０に送信し、当該端末ＩＤの中で、端末アドレス格納部２１内に端末アドレスが対応付けられているものを取得することにより、グループメンバ判定部３０５から受信したグループＩＤに対応するグループに属する通信端末５０の中で、現在ログイン中の通信端末５０の端末ＩＤを抽出する（Ｓ１０５）。

【００９４】

次に、鍵情報生成指示部３０１は、生成すべき鍵情報の有効期限を設定する。そして、鍵情報生成指示部３０１は、図９に示した鍵情報生成指示６１を生成し、生成した鍵情報生成指示６１を、グループメンバ判定部３０５を介してセッション管理サーバ４０へ送信する（Ｓ１０６）。そして、鍵情報生成指示部３０１は、送信した鍵情報生成指示６１を鍵情報生成指示格納部３００に格納し（Ｓ１０７）、通信条件登録部３０３は、再びステップ１００に示した処理を実行する。

【００９５】

通信開始要求に含まれる端末ＩＤが、データベース２０から取得した端末ＩＤに含まれ

ていない場合（Ｓ１０４：Ｎｏ）、グループメンバ判定部３０５は、当該端末ＩＤを含む通信開始拒否応答をネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信し（Ｓ１０８）、通信条件登録部３０３は、再びステップ１００に示した処理を実行する。

【００９６】

ステップ１０３において、通信開始要求を受信していない場合（Ｓ１０３：Ｎｏ）、鍵情報生成指示部３０１は、有効期限の経過前であって、現在時刻との差が所定値以下となる有効期限が鍵情報生成指示格納部３００内に存在するか否かを判定する（Ｓ１０９）。有効期限の経過前であって、現在時刻との差が所定値以下となる有効期限が鍵情報生成指示格納部３００内に存在する場合（Ｓ１０９：Ｙｅｓ）、鍵情報生成指示部３０１は、ステップ１０５から１０７に示した処理を実行することにより、鍵情報の再配布をセッション管理サーバ４０に指示する。この処理により、通信端末５０は、配付された鍵の有効期限が近づくと、自動的に鍵の配付を受けることができる。

【００９７】

有効期限の経過前であって、現在時刻との差が所定値以下となる有効期限が鍵情報生成指示格納部３００内に存在しない場合（Ｓ１０９：Ｎｏ）、グループメンバ判定部３０５は、通信終了要求を受信したか否かを判定する（Ｓ１１０）。通信終了要求を受信した場合（Ｓ１１０：Ｙｅｓ）、グループメンバ判定部３０５は、当該グループＩＤを含むグループメンバ取得要求をデータベース２０へ送信することにより、当該グループＩＤに対応付けられてグループメンバ情報格納部２３に格納されている端末ＩＤを取得する。そして、グループメンバ判定部３０５は、取得した端末ＩＤに基づいて、当該通信終了要求に含まれる端末ＩＤが、取得した端末ＩＤに含まれているか否かを判定する（Ｓ１１１）。

【００９８】

当該通信終了要求に含まれる端末ＩＤが、データベース２０から取得した端末ＩＤに含まれている場合（Ｓ１１１：Ｙｅｓ）、グループメンバ判定部３０５は、当該通信終了要求に含まれるグループＩＤおよびデータベース２０から取得した端末ＩＤを鍵情報削除指示部３０２へ送信する。

【００９９】

次に、鍵情報削除指示部３０２は、当該端末ＩＤを含むログイン中端末ＩＤ取得要求をデータベース２０へ送信することにより、当該端末ＩＤの中で、端末アドレス格納部２１内に端末アドレスが対応付けられているものを取得することにより、グループメンバ判定部３０５から受信したグループＩＤに対応するグループに属する通信端末５０の中で、現在ログイン中の通信端末５０の端末ＩＤを抽出する（Ｓ１１２）。そして、鍵情報削除指示部３０２は、抽出した端末ＩＤを含む鍵情報削除要求を生成し、生成した鍵情報削除要求を、グループメンバ判定部３０５を介してセッション管理サーバ４０へ送信する（Ｓ１１３）。

【０１００】

そして、鍵情報削除指示部３０２は、鍵情報生成指示格納部３００から受信したグループＩＤと、当該グループＩＤに対応付けて格納されている有効期限および端末ＩＤ一覧とを、鍵情報生成指示格納部３００から削除し（Ｓ１１４）、通信条件登録部３０３は、再びステップ１００に示した処理を実行する。

【０１０１】

当該通信終了要求に含まれる端末ＩＤが、データベース２０から取得した端末ＩＤに含まれていない場合（Ｓ１１１：Ｎｏ）、グループメンバ判定部３０５は、当該端末ＩＤを含む通信終了拒否応答をネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信し（Ｓ１１５）、通信条件登録部３０３は、再びステップ１００に示した処理を実行する。

【０１０２】

ステップ１１０において、通信終了要求を受信していない場合（Ｓ１１０：Ｎｏ）、通信条件削除部３０４は、管理ネットワーク１１を介して、セッション管理サーバ４０から

、通信条件削除要求を受信したか否かを判定する（Ｓ１１６）。通信条件削除要求６０を受信していない場合（Ｓ１１６：Ｎｏ）、通信条件登録部３０３は、再びステップ１００に示した処理を実行する。

【０１０３】

通信条件削除要求を受信した場合（Ｓ１１６：Ｙｅｓ）、通信条件削除部３０４は当該端末ＩＤをデータベース２０へ送信することにより、当該端末ＩＤおよび当該端末ＩＤに対応付けて格納されている通信条件を通信条件格納部２２から削除させる（Ｓ１１７）。そして、通信条件削除部３０４は、データベース２０から削除完了を示す応答を受信し、削除した通信条件に対応する端末ＩＤを含む削除完了通知を、ネットワークＩＦ部３０６を介してセッション管理サーバ４０へ送信し（Ｓ１１８）、通信条件登録部３０３は、再びステップ１００に示した処理を実行する。

【０１０４】

次に、グループ内暗号通信を実行する場合の暗号通信システム１０の動作の一例を、図１７を用いて説明する。

【０１０５】

まず、暗号通信システム１０は、グループ内暗号通信に参加するそれぞれの通信端末５０からの暗号通信路確立要求を処理して、当該通信端末５０の端末アドレスおよび通信条件をデータベース２０に登録する（Ｓ２０）。そして、グループ内でログイン中のいずれかの通信端末５０からの通信開始要求を処理することにより、暗号通信システム１０は、通信開始要求を送信した通信端末５０が属するグループにおいて、グループ内暗号通信を開始する（Ｓ３０）。そして、暗号通信システム１０は、時間の経過と共に、グループ内暗号通信で用いられている鍵情報を更新する（Ｓ４０）。

【０１０６】

次に、グループ内でログイン中のいずれかの通信端末５０からの通信終了要求を処理することにより、暗号通信システム１０は、通信終了要求を送信した通信端末５０が属するグループにおいて、グループ内暗号通信を終了する（Ｓ５０）。そして、暗号通信システム１０は、グループ内暗号通信への参加をやめるそれぞれの通信端末５０からの要求に応じて、当該通信端末５０の端末アドレスおよび通信条件をデータベース２０をデータベース２０から削除して、当該通信端末５０との暗号通信路を削除する（Ｓ６０）。

【０１０７】

以下、図１７に示したそれぞれのステップにおける暗号通信システム１０の詳細な動作について説明する。

【０１０８】

図１８は、ログイン処理（Ｓ２０）における暗号通信システム１０の詳細な動作の一例を示すシーケンス図である。

【０１０９】

まず、グループ内暗号通信に参加する通信端末５０のサーバ用暗号通信部５０３は、アプリケーション部５１０からの指示に従い、所有鍵格納部５０４に格納されている秘密鍵を用いて任意のメッセージに対するディジタル署名を生成し、生成したディジタル署名を、所有鍵格納部５０４に格納されている公開鍵証明書と共に、セッション管理サーバ４０へ送信することにより、セッション管理サーバ４０に、通信端末５０とセッション管理サーバ４０との間の暗号通信路確立を要求する。セッション管理サーバ４０の端末認証部４０９は、受信した暗号通信路確立要求に含まれている公開鍵証明書と、当該暗号通信路確立要求に含まれているメッセージに対するディジタル署名を検証することで、通信端末５０を認証する。（Ｓ２００）。

【０１１０】

認証に成功した場合、端末認証部４０９は、通信端末５０との暗号通信に用いる暗号鍵を鍵生成部４１１に生成させる（Ｓ２０１）。そして、端末認証部４０９は、所有鍵格納部４１２に格納されているセッション管理サーバ４０の秘密鍵を用いて、鍵生成部４１１によって生成された暗号鍵に対するディジタル署名を生成する。

【０１１１】
そして、端末認証部４０９は、暗号通信路確立要求に含まれる通信端末５０の公開鍵証明書を用いて、鍵生成部４１１によって生成された暗号鍵を暗号化し、暗号化した暗号鍵、生成したディジタル署名、および所有鍵格納部４１２に格納されているセッション管理サーバ４０の公開鍵証明書を含む応答を、暗号通信要求の送信元の通信端末５０へ送信する（Ｓ２０２）。そして、端末認証部４０９は、当該通信端末５０用の暗号鍵を暗号通信部４０８に設定する。
【０１１２】
次に、通信端末５０のサーバ用暗号通信部５０３は、所有鍵格納部５０４に格納されている秘密鍵を用いて、ステップ２０２で受信した応答に含まれる暗号化された暗号鍵を復号化することにより、暗号鍵を取得し、取得した暗号鍵を、セッション管理サーバ４０との間の暗号通信に用いる暗号鍵として設定する（Ｓ２０３）。
【０１１３】
次に、通信条件登録要求部５０９は、図８に示した通信条件登録要求６０をセッション管理サーバ４０へ送信する（Ｓ２０４）。端末アドレス登録部４０４は、通信条件登録要求６０に含まれる端末ＩＤおよび端末アドレスを含む端末アドレス登録要求を、管理ネットワーク１１を介してデータベース２０へ送信する（Ｓ２０５）。そして、データベース２０のデータベース制御部２６は、受信した端末アドレス登録要求に含まれる端末アドレスを、当該端末アドレス登録要求に含まれる端末ＩＤに対応付けて端末アドレス格納部２１に登録し、登録完了を示す応答を端末アドレス登録部４０４へ送信する（Ｓ２０６）。そして、通信条件登録要求転送部４０５は、管理ネットワーク１１を介して、通信条件登録要求６０を端末状態管理サーバ３０へ転送する（Ｓ２０７）。
【０１１４】
次に、端末状態管理サーバ３０の通信条件登録部３０３は、受信した通信条件登録要求６０に含まれる端末ＩＤおよび通信条件を含む通信条件登録指示を、管理ネットワーク１１を介してデータベース２０へ送信する（Ｓ２０８）。そして、データベース２０のデータベース制御部２６は、受信した通信条件登録指示に含まれる通信条件を、当該通信条件登録指示に含まれる端末ＩＤに対応付けて通信条件格納部２２に登録し、登録完了を示す応答を端末状態管理サーバ３０へ送信する（Ｓ２０９）。そして、通信条件登録部３０３は、登録完了を、管理ネットワーク１１を介してセッション管理サーバ４０に通知する（Ｓ２１０）。通信条件登録要求転送部４０５は、受信した登録完了通知をユーザネットワーク１２を介して通信端末５０へ転送する（Ｓ２１１）。
【０１１５】
図１９は、グループ内暗号通信開始処理（Ｓ３０）における暗号通信システム１０の詳細な動作の一例を示すシーケンス図である。
【０１１６】
まず、グループ内でログイン中の通信端末５０－１の通信開始要求部５０８は、ユーザネットワーク１２を介して、通信開始要求をセッション管理サーバ４０へ送信する（Ｓ３００）。通信要求転送部４０６は、ユーザネットワーク１２を介して受信した通信開始要求を、管理ネットワーク１１を介して端末状態管理サーバ３０へ転送する（Ｓ３０１）。
【０１１７】
グループメンバ判定部３０５は、受信した通信開始要求に含まれるグループＩＤを含むグループメンバ取得要求をデータベース２０へ送信する（Ｓ３０２）。そして、データベース制御部２６は、当該グループＩＤに対応するグループに属する通信端末５０の端末ＩＤをグループメンバ情報格納部２３から抽出し、抽出した端末ＩＤを含む応答を端末状態管理サーバ３０へ送信する（Ｓ３０３）。そして、グループメンバ判定部３０５は、データベース２０から取得した端末ＩＤの中に、通信開始要求に格納された端末ＩＤが含まれているか否かを判定する（Ｓ３０４）。
【０１１８】
そして、鍵情報生成指示部３０１は、ステップ３０３において取得した端末ＩＤを含む

ログイン中端末ＩＤ取得要求をデータベース２０へ送信する（Ｓ３０５）。そして、データベース制御部２６は、ログイン中端末ＩＤ取得要求に含まれる端末ＩＤの中で、端末アドレス格納部２１に端末アドレスが登録されているものを抽出し、抽出した端末ＩＤを含む応答を端末状態管理サーバ３０へ送信する（Ｓ３０６）。

【０１１９】

次に、鍵情報生成指示部３０１は、生成すべき鍵情報の有効期限を設定する。そして、鍵情報生成指示部３０１は、図９に示した鍵情報生成指示６１を生成し、生成した鍵情報生成指示６１を管理ネットワーク１１を介してセッション管理サーバ４０へ送信する（Ｓ３０７）。そして、鍵情報生成部４０２は、鍵情報生成指示６１に含まれる複数の端末ＩＤを含む通信条件取得要求をデータベース２０へ送信する（Ｓ３０８）。そして、データベース制御部２６は、通信条件取得要求に含まれる端末ＩＤに対応する通信条件を通信条件格納部２２から抽出し、抽出した通信条件を含む応答をセッション管理サーバ４０へ送信する（Ｓ３０９）。そして、鍵情報生成部４０２は、取得したそれぞれの通信端末５０の通信条件に共通の通信条件において実行可能な鍵を含む鍵情報を生成する（Ｓ３１０）。

【０１２０】

次に、鍵情報生成部４０２は、生成した鍵情報を含む配布鍵情報６２を生成し、生成した配布鍵情報６２を、グループ内暗号通信を行う通信端末５０－１、通信端末５０－２、および通信端末５０－３のそれぞれへ、ユーザネットワーク１２を介して送信する（Ｓ３１１、Ｓ３１２、Ｓ３１３）。これにより、グループ内暗号通信を行う通信端末５０－１、通信端末５０－２、および通信端末５０－３のそれぞれは、同一の配布鍵情報６２を共有することになる。そして、通信端末５０－１、通信端末５０－２、および通信端末５０－３のそれぞれは、受信した配布鍵情報６２に含まれる鍵を用いて、グループ内暗号通信を行う（Ｓ３１４）。具体的には、通信端末５０にインストールされているグループ内ネットワーク通信を行うアプリケーションが通信パケットを送受信する際に、端末用暗号通信部５０１は、鍵情報格納部５０５を検索して、そのパケットの通信先が図１０の配付鍵情報６２の端末アドレス６２２０あるいは、グループアドレス６２４に含まれているかどうか判定し、含まれていた場合には、鍵情報６２１を用いて、他の通信端末５０との間で暗号化パケットを送受信する。

【０１２１】

図２０は、鍵情報再配布処理（Ｓ４０）における暗号通信システム１０の詳細な動作の一例を示すシーケンス図である。

【０１２２】

鍵情報生成指示部３０１は、有効期限の経過前であって、現在時刻との差が所定値以下となる有効期限が鍵情報生成指示格納部３００内に存在する場合に、新たな有効期限を設定すると共に、当該有効期限に対応するグループＩＤおよび端末ＩＤ一覧を鍵情報生成指示格納部３００から抽出する。そして、鍵情報生成指示部３０１は、設定した有効期限と、鍵情報生成指示格納部３００から抽出したグループＩＤおよび端末ＩＤ一覧とを含む鍵情報再生成指示を生成し、生成した鍵情報再生成指示を管理ネットワーク１１を介してセッション管理サーバ４０へ送信する（Ｓ４００）。

【０１２３】

次に、鍵情報生成部４０２は、鍵情報再生成指示に含まれる複数の端末ＩＤを含む通信条件取得要求をデータベース２０へ送信する（Ｓ４０１）。そして、データベース制御部２６は、通信条件取得要求に含まれる端末ＩＤに対応する通信条件を通信条件格納部２２から抽出し、抽出した通信条件を含む応答をセッション管理サーバ４０へ送信する（Ｓ４０２）。そして、鍵情報生成部４０２は、取得したそれぞれの通信端末５０の通信条件に共通の通信条件において実行可能な鍵を含む鍵情報を生成する（Ｓ４０３）。そして、鍵情報生成部４０２は、生成した鍵情報を含む配布鍵情報６２を生成し、生成した配布鍵情報６２を、グループ内暗号通信を行っている通信端末５０－１、通信端末５０－２、および通信端末５０－３のそれぞれへ、ユーザネットワーク１２を介して配布する（Ｓ４０４

、Ｓ４０５、Ｓ４０６）。

【０１２４】

図２１は、グループ内暗号通信終了処理（Ｓ５０）における暗号通信システム１０の詳細な動作の一例を示すシーケンス図である。

【０１２５】

まず、グループ内暗号通信を実行中の通信端末５０－１の通信終了要求部５０６は、ユーザネットワーク１２を介して、通信終了要求をセッション管理サーバ４０へ送信する（Ｓ５００）。通信要求転送部４０６は、ユーザネットワーク１２を介して受信した通信終了要求を、管理ネットワーク１１を介して端末状態管理サーバ３０へ転送する（Ｓ５０１）。

【０１２６】

次に、グループメンバ判定部３０５は、受信した通信終了要求に含まれるグループＩＤを含むグループメンバ取得要求をデータベース２０へ送信する（Ｓ５０２）。そして、データベース制御部２６は、当該グループＩＤに対応するグループに属する通信端末５０の端末ＩＤをグループメンバ情報格納部２３から抽出し、抽出した端末ＩＤを含む応答を端末状態管理サーバ３０へ送信する（Ｓ５０３）。そして、グループメンバ判定部３０５は、データベース２０から取得した端末ＩＤの中に、通信終了要求に格納された端末ＩＤが含まれているか否かを判定する（Ｓ５０４）。

【０１２７】

そして、鍵情報生成指示部３０１は、ステップ５０３において取得した端末ＩＤを含むログイン中端末ＩＤ取得要求をデータベース２０へ送信する（Ｓ５０５）。そして、データベース制御部２６は、ログイン中端末ＩＤ取得要求に含まれる端末ＩＤの中で、端末アドレス格納部２１に端末アドレスが登録されているものを抽出し、抽出した端末ＩＤを含む応答を端末状態管理サーバ３０へ送信する（Ｓ５０６）。

【０１２８】

次に、鍵情報削除指示部３０２は、抽出した端末ＩＤを含む鍵情報削除指示を生成し、生成した鍵情報削除指示を管理ネットワーク１１を介してセッション管理サーバ４０へ送信する（Ｓ５０７）。そして、鍵情報削除要求送信部４０７は、鍵情報削除指示に含まれる複数の端末ＩＤで特定される端末５０のそれぞれへ、鍵情報削除要求を送信する（Ｓ５０８、Ｓ５０９、Ｓ５１０）。鍵情報削除要求を受信した通信端末５０－１、通信端末５０－２、および通信端末５０－３のそれぞれの鍵情報取得部５０２は、鍵情報削除要求に該当する鍵情報格納部５０５内の格納している鍵情報を削除する。

【０１２９】

なお、図２１のグループ内暗号通信終了処理は、通信端末５０以外から、要求することもできる。例えば、本暗号通信システム１０の管理者が、端末状態管理サーバ３０からグループ内暗号通信の中断を要求することもできる。その場合、図２１におけるＳ５００とＳ５０１が省略されることになる。

【０１３０】

図２２は、ログアウト処理（Ｓ６０）における暗号通信システム１０の詳細な動作の一例を示すシーケンス図である。

【０１３１】

まず、通信端末５０の通信条件削除要求部５０７は、自通信端末５０の端末ＩＤおよび端末アドレスを含む通信条件削除要求を、ユーザネットワーク１２を介してセッション管理サーバ４０へ送信する（Ｓ６００）。セッション管理サーバ４０の通信条件削除要求転送部４０１は、受信した通信条件削除要求を、管理ネットワーク１１を介して端末状態管理サーバ３０へ転送する（Ｓ６０１）。

【０１３２】

次に、端末状態管理サーバ３０の通信条件削除部３０４は、受信した通信条件削除要求に含まれる端末ＩＤを含む通信条件削除指示を、管理ネットワーク１１を介してデータベース２０へ送信する（Ｓ６０２）。そして、データベース２０のデータベース制御部２６

は、受信した通信条件削除指示に含まれる端末ＩＤに対応する通信条件を、通信条件格納部２２から削除し、削除した旨を含む応答を端末状態管理サーバ３０へ送信する（Ｓ６０３）。そして、通信条件削除部３０４は、削除した通信条件に対応する端末ＩＤを含む削除完了通知を、セッション管理サーバ４０へ送信する（Ｓ６０４）。

【０１３３】

次に、セッション管理サーバ４０の端末アドレス削除部４０３は、通信条件削除要求に含まれる端末アドレスを含む端末アドレス削除要求を、管理ネットワーク１１を介して、データベース２０へ送信する（Ｓ６０５）。そして、データベース２０のデータベース制御部２６は、受信した端末アドレス削除要求に含まれる端末アドレスを、端末アドレス格納部２１から削除し、削除した旨を含む応答を端末状態管理サーバ３０へ送信する（Ｓ６０６）。そして、端末アドレス削除部４０３は、削除完了通知を、当該通信条件削除要求を送信してきた通信端末５０へ送信する（Ｓ６０７）。

【０１３４】

次に、サーバ用暗号通信部５０３は、ユーザネットワーク１２を介してセッション管理サーバ４０へ、暗号通信路削除要求を送信する（Ｓ６０８）。そして、セッション管理サーバ４０の端末認証部４０９は、暗号通信路削除要求に対する応答を、当該暗号通信路削除要求を送信してきた通信端末５０へ送信する（Ｓ６０９）。そして、通信端末５０は、セッション管理サーバ４０と共有していた暗号鍵を破棄し（Ｓ６１０）、セッション管理サーバ４０は、通信端末５０と共有していた暗号鍵を削除する（Ｓ６１１）。

【０１３５】

上記説明から明らかなように、本実施形態の暗号通信システム１０によれば、グループ内の暗号通信に用いられる鍵や設定情報を配布することにより発生するトラフィックをより少なくすることができる。また、グループ内暗号通信に用いられる鍵情報と共に、グループに属している通信端末５０であって、現在ログイン中の通信端末５０に関する情報が配布されるので、それぞれの通信端末５０は、グループ内暗号通信に参加している他の通信端末５０を認識することができる。

【０１３６】

なお、本発明は、上記の各実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【０１３７】

例えば、上記した実施形態では、セッション管理サーバ４０と当該通信端末５０との間で暗号鍵が共有された後に、セッション管理サーバ４０によって、データベース２０の端末アドレス格納部２１に当該通信端末５０の端末アドレスが登録されると共に、端末状態管理サーバ３０を介して、通信条件格納部２２に当該通信端末５０の通信条件が登録されることをログインの一例として説明したが、本発明はこれに限られない。

【０１３８】

ログインとは、暗号通信システム１０によって提供されるグループ内暗号通信サービスに、通信端末５０が参加することを意味すればよい。例えば、セッション管理サーバ４０によって、データベース２０の端末アドレス格納部２１に当該通信端末５０の端末アドレスが登録されること、または、セッション管理サーバ４０によって、端末状態管理サーバ３０を介して、通信条件格納部２２に当該通信端末５０の通信条件が登録されることがログインと定義されてもよい。

【０１３９】

また、上記した実施形態では、データベース２０、端末状態管理サーバ３０、およびセッション管理サーバ４０をそれぞれ独立した装置として説明したが、本発明はこれに限られず、データベース２０、端末状態管理サーバ３０、およびセッション管理サーバ４０が１台の装置内で実現されていてもよく、データベース２０、端末状態管理サーバ３０、およびセッション管理サーバ４０のそれぞれに含まれるそれぞれの機能が、２台以上の装置のそれぞれに分散させて実現されていてもよい。

【０１４０】

また、上記した実施形態では、端末アドレスとしてＩＰｖ４を例に説明したが、本発明はこれに限られず、ＩＰｖ６においても同様に本発明を適用することができる。例えば、ＩＰｖ４を例に説明した上記の実施形態におけるマルチキャストアドレスは、ＩＰｖ６におけるエニイキャストアドレスに対しても同様に適用することができる。

【０１４１】

また、上記した実施形態において、端末状態管理サーバ３０は、通信開始要求を受信した場合に、当該通信開始要求に含まれるグループＩＤに基づき、データベース２０内のグループメンバ情報格納部２３を参照して、グループに属する通信端末５０の端末ＩＤを取得したが、本発明はこれに限られない。

【０１４２】

端末状態管理サーバ３０は、例えば、グループ内暗号通信を行うネットワークのネットワークアドレスと、当該グループ内暗号通信をブロードキャストによって実行する旨と、通信開始要求の送信元の通信端末５０の端末ＩＤとを含む通信開始要求を受信した場合に、当該ネットワークアドレスに属する通信端末５０の端末ＩＤを、データベース２０の端末アドレス格納部２１から抽出することにより、グループ内暗号通信の対象となる通信端末５０の端末ＩＤを抽出するようにしてもよい。

【０１４３】

また、上記した実施形態において、暗号通信システム１０は、グループ内暗号通信を行うグループをグループＩＤを用いて管理しており、それぞれの通信端末５０には、グループ内暗号通信を行うグループのグループＩＤが予め設定されている場合を例に説明したが、本発明はこれに限られない。

【０１４４】

例えば、管理ネットワーク１１およびユーザネットワーク１２に接続される名前解決サーバが設けられ、当該名前解決サーバが、複数の通信端末５０の端末ＩＤ含むグループＩＤ取得要求を、ユーザネットワーク１２を介して通信端末５０から受信した場合に、管理ネットワーク１１を介してデータベース２０のグループメンバ情報格納部２３を参照することにより、対応するグループＩＤを取得し、取得したグループＩＤを、当該グループＩＤ取得要求の送信元の通信端末５０へ送信するようにしてもよい。

【０１４５】

なお、上記の名前解決サーバは、複数の通信端末５０の端末アドレスを含むグループＩＤ取得要求を、ユーザネットワーク１２を介して通信端末５０から受信した場合に、管理ネットワーク１１を介してデータベース２０の端末アドレス格納部２１とグループメンバ情報格納部２３を参照することにより、対応するグループＩＤを取得し、取得したグループＩＤを、当該グループＩＤ取得要求の送信元の通信端末５０へ送信してもよい。

【０１４６】

また、上記の名前解決サーバは、グループアドレス（例えば、マルチキャストアドレスやブロードキャストアドレス）を含むグループＩＤ取得要求を、ユーザネットワーク１２を介して通信端末５０から受信した場合に、管理ネットワーク１１を介してデータベース２０のグループアドレス格納部２４を参照することにより、対応するグループＩＤを取得し、取得したグループＩＤを、当該グループＩＤ取得要求の送信元の通信端末５０へ送信してもよい。

【０１４７】

このように、それぞれの通信端末５０は、グループ内暗号通信を行う複数の通信端末５０の端末ＩＤまたは端末アドレスを、ユーザネットワーク１２を介して当該名前解決サーバに問い合わせることにより、当該グループ内暗号通信を行うグループのグループＩＤを取得することができる。これにより、それぞれの通信端末５０は、グループＩＤを予め記憶しておく必要がなくなる。さらに、暗号通信システム１０は、データベース２０内のグループメンバ情報格納部２３において、それぞれのグループに属する通信端末５０の管理を一括して行うことができるので、グループ内の通信端末５０の追加や削除をより柔軟に行うことができる。

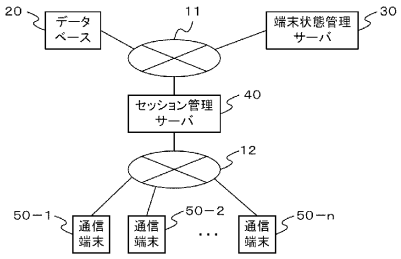
【０１４８】
なお、上記した名前解決サーバが、データベース２０内のグループメンバ情報格納部２３とは別個に、グループメンバ情報格納部２３を有し、通信端末５０からのグループＩＤ取得要求に対して、自身が格納しているグループメンバ情報格納部２３を参照して、対応するグループＩＤを返信するようにしても、本発明における効果を得ることができることはいうまでもない。
【０１４９】
また、上記した実施形態において、セッション管理サーバ４０は、端末状態管理サーバ３０からの指示に応じて生成した鍵情報を、当該鍵情報を用いてグループ内暗号通信を行うグループに属する通信端末５０であって、現在ログイン中の通信端末５０の全てに配布するが、本発明はこれに限られない。例えば、図１９のステップ３０７において、端末状態管理サーバ３０から鍵情報生成指示６１を受信した場合に、セッション管理サーバ４０の鍵情報生成部４０２は、当該鍵情報生成指示６１内の端末ＩＤ一覧６１３に含まれるそれぞれの端末ＩＤ６１３０について、当該端末ＩＤ６１３０に対応する通信端末５０へ、今回のグループ内暗号通信に参加するか否かを問い合わせるようにしてもよい。
【０１５０】
この場合、鍵情報生成部４０２は、参加する旨の応答を受信した通信端末５０のそれぞれについて、通信条件格納部２２から取得した通信条件に基づいて鍵情報を生成し、生成した鍵情報を含み、かつ、参加する旨の応答を受信した通信端末５０の端末ＩＤ一覧および端末アドレス一覧等を含む配布鍵情報６２を生成する。そして、鍵情報生成部４０２は、生成した配布鍵情報６２を、グループ内暗号通信に参加する旨の応答を送信したそれぞれの通信端末５０へ送信する。これにより、暗号通信システム１０は、鍵情報の配布によって発生するトラフィックをさらに少なくすることができる。
【０１５１】
また、鍵情報生成部４０２は、鍵情報の再配布指示を端末状態管理サーバ３０から受信した場合にも、当該鍵情報再配布指示内の端末ＩＤ一覧に含まれるそれぞれの端末ＩＤについて、当該端末ＩＤに対応する通信端末５０へ、グループ内暗号通信に継続して参加するか否かを問い合わせるようにしてもよい。
【図面の簡単な説明】
【０１５２】
【図１】本発明の一実施形態に係る暗号通信システム１０の構成を示すシステム構成図である。
【図２】データベース２０の詳細な機能構成を例示するブロック図である。
【図３】端末アドレス格納部２１に格納されるデータ構造を例示する説明図である。
【図４】通信条件格納部２２に格納されるデータ構造を例示する説明図である。
【図５】グループメンバ情報格納部２３に格納されるデータ構造を例示する説明図である。
【図６】グループアドレス格納部２４に格納されるデータ構造を例示する説明図である。
【図７】セッション管理サーバ４０の詳細な機能構成を例示するブロック図である。
【図８】通信条件登録要求６０に含まれるデータを例示する説明図である。
【図９】鍵情報生成指示６１に含まれるデータを例示する説明図である。
【図１０】配布鍵情報６２に含まれるデータを例示する説明図である。
【図１１】端末状態管理サーバ３０の詳細な機能構成を例示するブロック図である。
【図１２】鍵情報生成指示格納部３００に格納されるデータ構造を例示する説明図である。
【図１３】通信端末５０の詳細な機能構成を例示するブロック図である。
【図１４】通信条件格納部５１１に格納されるデータ構造を例示する説明図である。
【図１５】データベース２０、端末状態管理サーバ３０、またはセッション管理サーバ４０の機能を実現する情報処理装置７０のハードウェア構成を例示するハードウェア構成図である。

【図１６】端末状態管理サーバ３０の動作を例示するフローチャートである。
【図１７】暗号通信システム１０の動作を例示するフローチャートである。
【図１８】ログイン処理（Ｓ２０）における暗号通信システム１０の詳細な動作を例示するシーケンス図である。
【図１９】グループ内暗号通信開始処理（Ｓ３０）における暗号通信システム１０の詳細な動作を例示するシーケンス図である。
【図２０】鍵情報再配布処理（Ｓ４０）における暗号通信システム１０の詳細な動作を例示するシーケンス図である。
【図２１】グループ内暗号通信終了処理（Ｓ５０）における暗号通信システム１０の詳細な動作を例示するシーケンス図である。
【図２２】ログアウト処理（Ｓ６０）における暗号通信システム１０の詳細な動作を例示するシーケンス図である。
【符号の説明】
【０１５３】
１０・・・暗号通信システム、１１・・・管理ネットワーク、１２・・・ユーザネットワーク、２０・・・データベース、２１・・・端末アドレス格納部、２２・・・通信条件格納部、２３・・・グループメンバ情報格納部、２４・・・グループアドレス格納部、２５・・・ネットワークＩＦ部、３０・・・端末状態管理サーバ、３００・・・鍵情報生成指示格納部、３０１・・・鍵情報生成指示部、３０２・・・鍵情報削除指示部、３０３・・・通信条件登録部、３０４・・・通信条件削除部、３０５・・・グループメンバ判定部、３０６・・・ネットワークＩＦ部、４０・・・セッション管理サーバ、４００・・・ネットワークＩＦ部、４０１・・・通信条件削除要求転送部、４０２・・・鍵情報生成部、４０３・・・端末アドレス削除部、４０４・・・端末アドレス登録部、４０５・・・通信条件登録要求転送部、４０６・・・通信要求転送部、４０７・・・鍵情報削除要求送信部、４０８・・・暗号通信部、４０９・・・端末認証部、４１０・・・ネットワークＩＦ部、４１１・・・鍵生成部、４１２・・・所有鍵格納部、５０・・・通信端末、５００・・・ネットワークＩＦ部、５０１・・・端末用暗号通信部、５０２・・・鍵情報取得部、５０３・・・サーバ用暗号通信部、５０４・・・所有鍵格納部、５０５・・・鍵情報格納部、５０６・・・通信終了要求部、５０７・・・通信条件削除要求部、５０８・・・通信開始要求部、５０９・・・通信条件登録要求部、５１０・・・アプリケーション部、５１１・・・通信条件格納部、６０・・・通信条件登録要求、６１・・・鍵情報生成指示、６２・・・配布鍵情報、７０・・・情報処理装置、７１・・・ＣＰＵ、７２・・・ＲＡＭ、７３・・・ＲＯＭ、７４・・・ＨＤＤ、７５・・・通信インターフェイス、７６・・・入出力インターフェイス、７７・・・メディアインターフェイス、７８・・・記録媒体

【図１】

図1

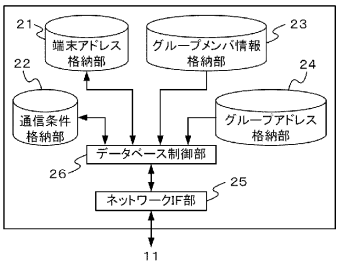
暗号通信システム10



【図２】

図2

データベース20



【図３】

図3

端末アドレス格納部21

210 端末ID	211 端末アドレス
m1@***.***	***.***.***.***
m2@***.***	***.***.***.***
m3@***.***	***.***.***.***
⋮	⋮

【図４】

図4

通信条件格納部22

220 端末ID	221 暗号アルゴリズム	222 鍵長	223 ハッシュ関数種別	…	224 優先順位
m1@***.***	＊＊＊	＊＊	＊＊＊	…	1
	＊＊＊	＊＊	＊＊＊	…	2
	＊＊＊	＊＊	＊＊＊	…	3
	⋮	⋮	⋮	⋮	⋮
m2@***.***	＊＊＊	＊＊	＊＊＊	…	1
	＊＊＊	＊＊	＊＊＊	…	2
	＊＊＊	＊＊	＊＊＊	…	3
	⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮	⋮

【図５】

図5

グループメンバ情報格納部23

230 グループID	231 端末ID
g1@***.***	m1@***.***
	m2@***.***
	m3@***.***
	⋮
g2@***.***	m4@***.***
	m5@***.***
	⋮
⋮	⋮

【図６】

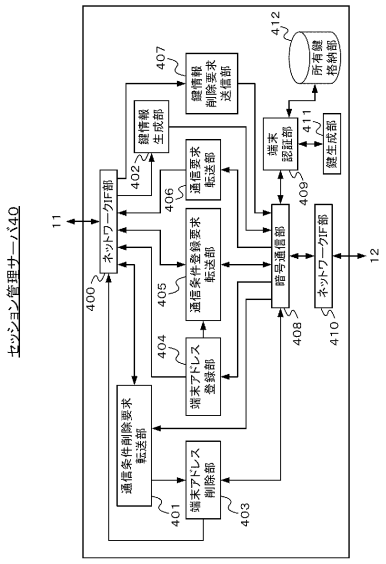
図6

グループアドレス格納部24

240 グループID	241 グループアドレス
g1@***.***	224.***.***.***
g2@***.***	192.168.10.255
⋮	⋮

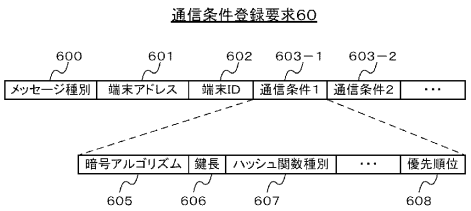
【図７】

図7



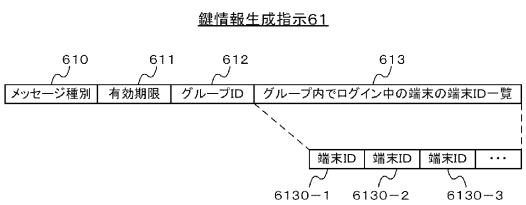
【図８】

図8



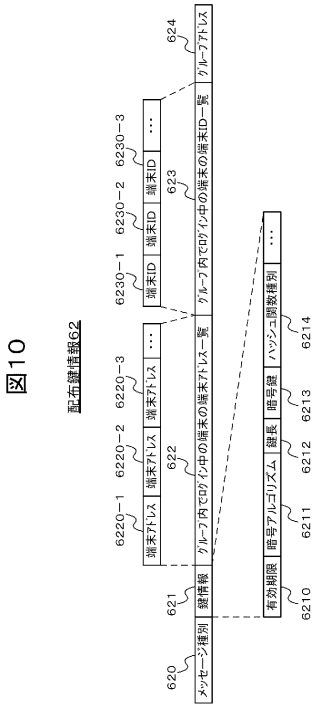
【図９】

図9



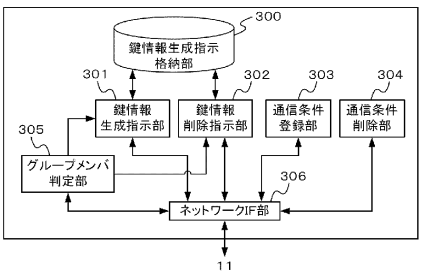
【図１０】

図10



【図１１】

図11



【図１２】

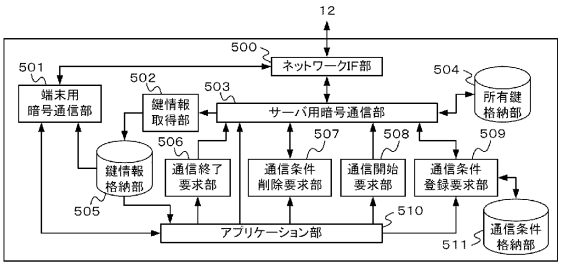
図12

鍵情報生成指示格納部300

3000 有効期限	3001 グループID	3002 グループ内でログイン中の端末の端末ID一覧
＊＊＊	＊＊＊	＊＊＊
＊＊＊	＊＊＊	＊＊＊
：	：	⋮

【図１３】

図13



【図１４】

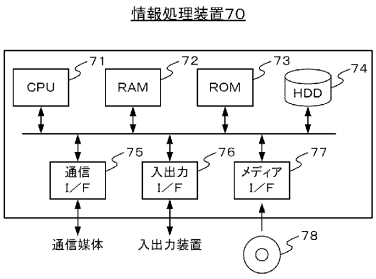
図14

通信条件格納部511

5110 暗号アルゴリズム	5111 鍵長	5112 ハッシュ関数種別	…	5113 優先順位
＊＊＊	＊＊	＊＊＊	…	1
＊＊＊	＊＊	＊＊＊	…	2
＊＊＊	＊＊	＊＊＊	…	3
：	：	：	⋮	⋮

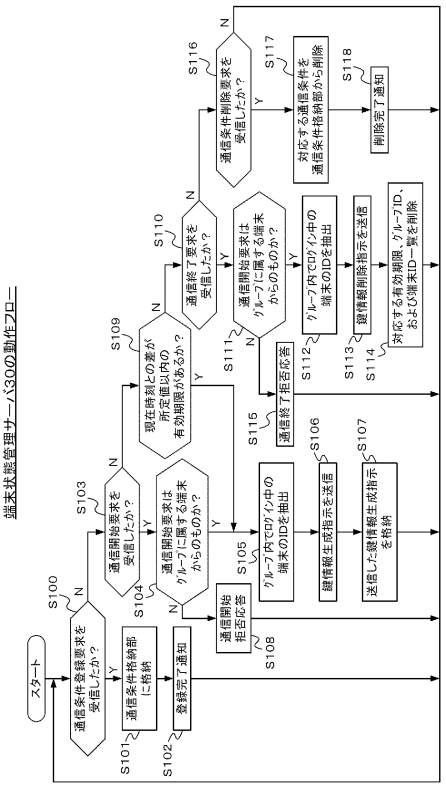
【図１５】

図15



【図１６】

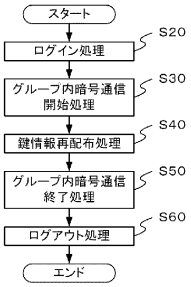
図16



【図１７】

図17

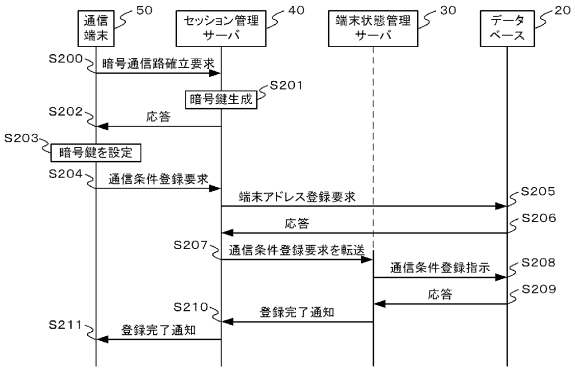
暗号通信システム10の動作フロー



【図１８】

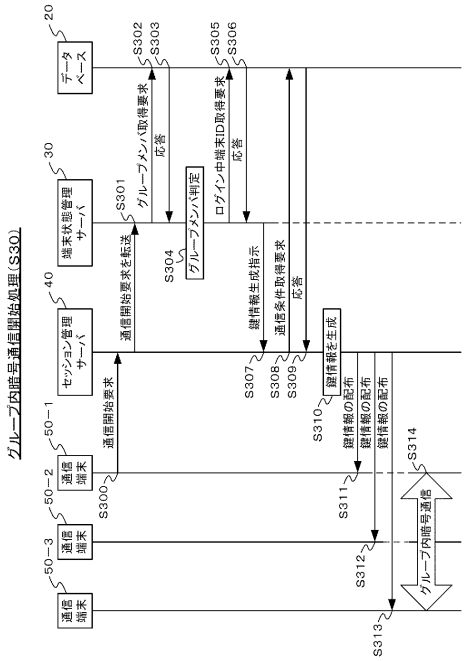
図18

ログイン処理（S20）



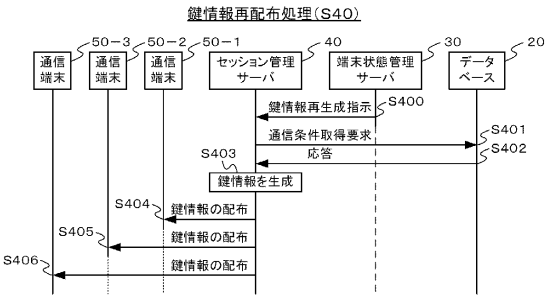
【図１９】

図19



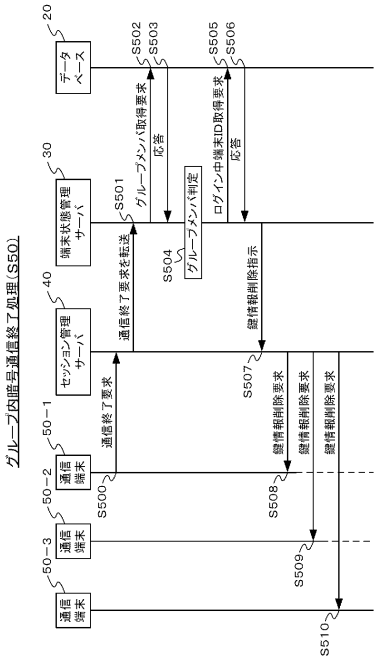
【図２０】

図20



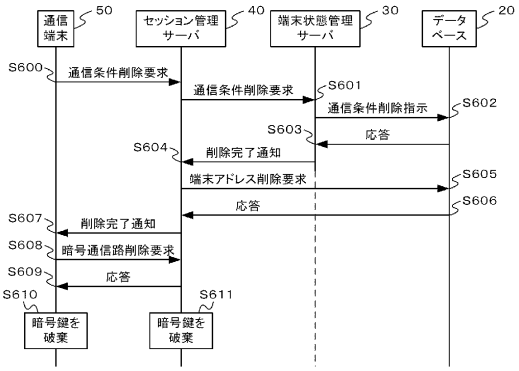
【図２１】

図21



【図２２】

図22



フロントページの続き

(72)発明者　藤城　孝宏
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　星野　和義
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ネットワークソリューション事業部内
(72)発明者　竹内　敬亮
東京都国分寺市東恋ヶ窪一丁目２８０番地　株式会社日立製作所　中央研究所内

審査官　青木　重徳

(56)参考文献　特開２００４－０２３２３７（ＪＰ，Ａ）
特表２００５－５００７１４（ＪＰ，Ａ）
特開２００５－２３６８５０（ＪＰ，Ａ）
特開２０００－１０６５５２（ＪＰ，Ａ）
高田治，澤井裕子，星野和義，鍛忠司，竹内敬亮，藤城孝宏，手塚悟，“セキュアサービスプラットフォームにおけるセキュア通信の状態検知”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００５年　7月１５日，Ｖｏｌ．１０５，Ｎｏ．１９４，ｐ．５３－５８
鍛忠司，高田治，星野和義，藤城孝宏，手塚悟，“セキュアサービスプラットフォームにおけるセキュア通信確立モデル”，情報処理学会研究報告，日本，社団法人情報処理学会，２００５年　3月２３日，Ｖｏｌ．２００５，Ｎｏ．３３，ｐ．１５１－１５６
細木正司，田中智博，永岡孝，“セキュアサービスプラットフォームでのセキュリティ状態を用いたアクセス制御に関する検討”，電子情報通信学会２００５年総合大会講演論文集，日本，社団法人電子情報通信学会，２００５年　3月　7日，通信2，Ｂ－７－１７，ｐ．１７１
渡辺龍，窪田歩，田中俊昭，“セキュアサービスプラットフォームにおけるプライバシー保護を考慮したＩＤ生成管理方式の実装”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００５年　5月１９日，Ｖｏｌ．１０５，Ｎｏ．８６，ｐ．１７－２０

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０６Ｆ　２１／２０