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

特許第3644579号
(P3644579)

(45)発行日　平成17年4月27日(2005.4.27)　(24)登録日　平成17年2月10日(2005.2.10)

(51)Int.Cl.[7]	F I		
H04L 9/08	H04L	9/00	601C
G06F 13/00	G06F	13/00	351Z
	H04L	9/00	601E
	H04L	9/00	601A

請求項の数 22　(全 25 頁)

(21)出願番号　特願平10-308007
(22)出願日　平成10年10月29日(1998.10.29)
(65)公開番号　特開2000-134193(P2000-134193A)
(43)公開日　平成12年5月12日(2000.5.12)
審査請求日　平成13年10月29日(2001.10.29)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100094145
弁理士　小野　由己男
(74)代理人　100094167
弁理士　宮川　良夫
(74)代理人　100106367
弁理士　稲積　朋子
(72)発明者　松本　達郎
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】セキュリティ強化方法及び装置

(57)【特許請求の範囲】

【請求項１】

互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置に用いられ、

前記通信装置の処理手段が、前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を記憶手段に保持する記憶ステップと、

前記処理手段が、通信内容を前記通信装置から取得し、前記暗号鍵を用いて暗号化する暗号化ステップと、

前記処理手段が、通信内容を前記通信装置から取得し、前記暗号鍵を用いて復号化する復号化ステップと、

前記通信装置が前記いずれかのネットワークに参加している場合に、前記処理手段が、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を前記通信装置から取得し、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を前記取得した利用者情報に基づいて設定し、取得した利用者情報及び設定した鍵配布属性を前記記憶手段に格納する利用者管理ステップと、

前記処理手段が、前記設定した鍵配布属性に基づいて前記暗号鍵を取得するか否かを判断し、前記判断の結果に基づいて前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する鍵取得ステップと、

前記処理手段が、前記設定した鍵配布属性に基づいて前記暗号鍵を生成するか否かを判断し、前記判断の結果に基づいて前記暗号鍵を生成し、他の前記通信装置から前記暗号鍵

の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能な鍵配布ステップと、

を含むセキュリティ強化方法。

【請求項２】

他の通信装置と互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置とともに用いられ、

前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する記憶手段と、

通信内容を前記通信装置から取得し、前記暗号鍵を用いて暗号化する暗号化手段と、

通信内容を前記通信装置から取得し、前記暗号鍵を用いて復号化する復号化手段と、

前記通信装置が前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を前記通信装置から取得し、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を、前記取得した利用者情報に基づいて設定し、取得した利用者情報及び設定した鍵配布属性を前記記憶手段に格納する利用者管理手段と、

前記設定した鍵配布属性に基づいて前記暗号鍵を取得するか否かを判断し、前記判断の結果に基づいて前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する鍵取得手段と、

前記設定した鍵配布属性に基づいて前記暗号鍵を生成するか否かを判断し、前記判断の結果に基づいて前記暗号鍵を生成し、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能な鍵配布手段と、

を備えるセキュリティ強化装置。

【請求項３】

前記通信装置は、前記セキュリティ強化装置との連携手段を有し、

前記連携手段は、前記暗号鍵の要求、前記要求に応じて送信される暗号鍵、前記利用者情報に関する情報及び所定の条件に合致する場合は通信内容の受け渡しを、前記通信装置とセキュリティ強化装置との間で行う、請求項２に記載のセキュリティ強化装置。

【請求項４】

前記利用者管理手段は、所定の条件に基づいて、他の通信装置を選択し、前記暗号鍵の配布を許可する鍵配布属性を前記他の通信装置に付与し、かつ鍵配布属性の設定及び設定対象の通信装置を前記通信装置から取得し、前記記憶手段に格納する、請求項２に記載のセキュリティ強化装置。

【請求項５】

前記利用者管理手段は、他の通信装置の選択と、前記暗号鍵の配布を許可する鍵配布属性の前記他の通信装置への付与及び解除の指示とを受け付け、かつ鍵配布属性の設定及び設定対象の通信装置を前記通信装置から取得し、前記記憶手段に格納する、請求項２に記載のセキュリティ強化装置。

【請求項６】

前記鍵取得手段は、所定の条件に基づいて前記暗号鍵の要求先を選択する、請求項２に記載のセキュリティ強化装置。

【請求項７】

前記鍵取得手段は、所定の条件に基づいて前記暗号鍵の要求先を選択して前記暗号鍵を要求し、所定時間内に前記要求先から暗号鍵が送信されない場合、他の通信装置を選択して再度要求を行う、請求項２に記載のセキュリティ強化装置。

【請求項８】

前記鍵取得手段は、前記通信内容が暗号化されている場合に前記暗号鍵の取得要求を行う、請求項２に記載のセキュリティ強化装置。

【請求項９】

前記復号化手段は、前記通信装置から受け取る通信内容を復号不可能と判断した場合、前記暗号鍵の要求を行うことを決定し、
前記鍵取得手段は、前記復号化手段の決定に従い、前記暗号鍵の取得要求を行う、請求項２に記載のセキュリティ強化装置。
【請求項１０】
前記記憶手段は、複数の暗号鍵と暗号鍵を特定する鍵識別情報とを対応付けて記憶し、
前記暗号化手段は、前記通信内容の暗号化に用いられた暗号鍵を示す鍵識別情報と通信内容とを、前記通信装置を介してネットワークに送出可能であり、
前記復号化手段は、前記鍵識別情報で特定される暗号鍵が前記記憶手段に保持されているか否かを判断し、
前記鍵取得手段は、前記判断結果に従い、前記鍵識別情報を通知して前記暗号鍵の取得要求を行う、請求項２に記載のセキュリティ強化装置。
【請求項１１】
前記鍵取得手段は、利用者の公開鍵暗号系の公開鍵を前記暗号鍵の要求とともに通知し、前記要求に応じて送信される暗号鍵を利用者の秘密鍵を用いて復号化し、
前記鍵配布手段は、前記要求元の公開鍵暗号系の公開鍵を用いて暗号化した前記暗号鍵を配布する、
請求項２に記載のセキュリティ強化装置。
【請求項１２】
前記鍵配布手段は、他の前記通信装置から前記暗号鍵の要求があった場合、前記要求を検証し、検証結果に基づいて前記記憶手段からいずれかの暗号鍵を読み出し、前記他の通信端末に配布可能である、請求項２に記載のセキュリティ強化装置。
【請求項１３】
所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備える、請求項２に記載のセキュリティ強化装置。
【請求項１４】
所定のタイミングで前記暗号鍵を更新し、前記更新した暗号鍵を直前の暗号鍵を用いて暗号化して他の通信装置に配布する鍵変更手段をさらに備える、請求項２に記載のセキュリティ強化装置。
【請求項１５】
前記鍵変更手段は、前記各通信装置内に保持される秘密情報、時間情報及びネットワークに固有の情報のいずれかまたは全ての組合せに基づいて前記暗号鍵を生成する、請求項２に記載のセキュリティ強化装置。
【請求項１６】
前記鍵変更手段は、前記各通信装置内に保持される秘密情報、時間情報及びネットワークに固有の情報のいずれかの組合せまたは全てを、一方向関数で暗号化して前記暗号鍵を生成する、請求項２に記載のセキュリティ強化装置。
【請求項１７】
前記利用者管理手段は、前記暗号鍵の更新及び配布を許可する鍵変更属性を、前記取得した利用者情報に基づいて設定して前記記憶手段に格納し、
前記鍵変更属性の有無に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備える、請求項２に記載のセキュリティ強化装置。
【請求項１８】
前記利用者管理手段は、
利用者が前記暗号鍵の更新及び配布を許可する鍵変更属性を有する場合に、所定の条件に基づいて他の通信装置を選択し、前記選択した通信装置に前記鍵変更属性を設定可能であり、
かつ鍵変更属性の設定及び設定対象の通信装置を前記通信装置から取得して前記記憶手段に格納し、
前記鍵変更属性の有無に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信

装置に配布する鍵変更手段をさらに備える、
請求項２に記載のセキュリティ強化装置。
【請求項１９】
前記利用者管理手段は、前記暗号鍵の更新及び配布を許可する鍵変更属性及び優先順位を、前記取得した利用者情報に基づいて設定して前記記憶手段に格納し、前記利用者情報の変化に従って前記優先順位の書き換えを行い、
前記鍵変更属性及び優先順位に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備える、請求項２に記載のセキュリティ強化装置。
【請求項２０】
前記利用者管理手段は、
利用者が前記暗号鍵の更新及び配布を許可する鍵変更属性を有する場合に、所定の条件に基づいて他の通信装置を選択し、前記他の通信装置に前記鍵変更属性と優先順位とを設定可能であり、
かつ鍵変更属性と優先順位との設定及び設定対象の通信装置を前記通信装置から取得して前記記憶手段に格納し、前記利用者情報の変化に従って前記優先順位の書き換えを行い、
前記鍵変更属性及び優先順位に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備える、
請求項２に記載のセキュリティ強化装置。
【請求項２１】
互いに同一のネットワークを共有して同時に双方向通信が可能な複数の通信装置から構成され、
前記各通信装置は、
前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する記憶手段と、
通信内容を前記暗号鍵を用いて暗号化する暗号化手段と、
通信内容を前記暗号鍵を用いて復号化する復号化手段と、
前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を取得し、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を、前記取得した利用者情報に基づいて設定し、取得した利用者情報及び設定した鍵配布属性を前記記憶手段に格納する利用者管理手段と、
前記設定した鍵配布属性に基づいて前記暗号鍵を取得するか否かを判断し、前記判断の結果に基づいて前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する鍵取得手段と、
前記設定した鍵配布属性に基づいて前記暗号鍵を生成するか否かを判断し、前記判断の結果に基づいて前記暗号鍵を生成し、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能な鍵配布手段と、
を備えるセキュリティ強化システム。
【請求項２２】
互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置に用いられる、セキュリティ強化プログラムを記録したコンピュータ読み取り可能な記録媒体であって、
前記通信装置の処理手段が、前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を記憶手段に保持する記憶段階と、
前記処理手段が、通信内容を前記通信装置から取得し、前記暗号鍵を用いて暗号化する暗号化段階と、

前記処理手段が、通信内容を前記通信装置から取得し、前記暗号鍵を用いて復号化する復号化段階と、

前記通信装置が前記いずれかのネットワークに参加している場合に、前記処理手段が、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を前記通信装置から取得し、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を前記取得した利用者情報に基づいて設定し、取得した利用者情報及び設定した鍵配布属性を前記記憶手段に格納する利用者管理段階と、

前記処理手段が、前記設定した鍵配布属性に基づいて前記暗号鍵を取得するか否かを判断し、前記判断の結果に基づいて前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する鍵取得段階と、

前記処理手段が、前記設定した鍵配布属性に基づいて前記暗号鍵を生成するか否かを判断し、前記判断の結果に基づいて前記暗号鍵を生成し、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能な鍵配布段階と、

を実行させるための、セキュリティ強化プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、イントラネットやインターネットなどのコンピュータネットワーク上で行われる通信のセキュリティを高める技術に関し、なかでもチャットシステムにおける会話内容のセキュリティを高める技術に関する。

本発明において、チャットシステムとは、チャットサーバと複数のチャットクライアントとから構成され、複数の利用者が互いに同一のチャネルを共有して同時に会話可能なシステムをいう。チャネルとは、論理的にユーザをグルーピングした仮想空間であり、チャネル内での発言がチャネルを共有する利用者全員にブロードキャストされる仮想空間である。ニックネームとは、チャットシステム上でユーザを識別するための名前である。チャネルオペレータ属性とは、チャネル内のユーザ管理及びモード管理を行う権限である。ボットとは、チャネルに参加して様々なサービスを提供するソフトウェアロボットを言う。

【０００２】

【従来の技術】

従来、チャットサーバとチャットクライアントとからなるチャットシステムにおいて、チャットクライアント間の会話内容のセキュリティを高めるために、会話内容を共通鍵で暗号化することが提案されている。この共通鍵の生成方法として、例えばチャットサーバがチャネル暗号鍵を生成し、複数のチャットクライアントに配布する方法が提供されている。

【０００３】

また、チャットクライアントとしてサーバに接続するボットを準備しておき、このボットにチャネル暗号鍵を生成及び配布させ、また生成したチャネル暗号鍵を管理させる方法も提案されている。さらに、チャットクライアントにあらかじめチャネル暗号鍵を組み込んでおくことも考えられる。

【０００４】

【発明が解決しようとする課題】

前記チャットサーバがチャネル暗号鍵を生成してチャットクライアントに配布する方法では、クライアントとサーバとの間の通信路上では会話内容の秘匿が行われる。しかし、サーバがチャネル暗号鍵を知っているので、サーバ上で会話の解読が可能であるという問題がある。

【０００５】

一方、ボットを用いてチャネル鍵を管理する方法を用いると、チャットサーバに会話内

容が漏洩することはないものの、ボット上で会話内容の解読が可能である。また、サーバと別個独立したボットを運用することになり、運用上面倒である。チャットクライアントにチャネル暗号鍵を組み込む構成は、単純ではあるものの鍵を変更できないため、鍵を解読される可能性が高くなるおそれがある。

【０００６】

本発明は、チャネル暗号鍵を用いて会話の暗号化／復号化を行う場合に、チャネル暗号鍵を管理する負担を軽減し、チャネル鍵の解読を困難にするセキュリティ強化方法及び装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】

前記の課題を解決するために、本願第１発明は、互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置に用いられ、以下のステップを含むセキュリティ強化方法を提供する。

・前記通信装置の処理手段が、前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を記憶手段に保持する記憶ステップ、

・前記処理手段が、通信内容を前記通信装置から取得し、前記暗号鍵を用いて暗号化する暗号化ステップ、

・前記処理手段が、通信内容を前記通信装置から取得し、前記暗号鍵を用いて復号化する復号化ステップ、

・前記通信装置が前記いずれかのネットワークに参加している場合に、前記処理手段が、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を前記通信装置から取得し、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を前記取得した利用者情報に基づいて設定し、取得した利用者情報及び設定した鍵配布属性を前記記憶手段に格納する利用者管理ステップ、

・前記処理手段が、前記設定した鍵配布属性に基づいて前記暗号鍵を取得するか否かを判断し、前記判断の結果に基づいて前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する鍵取得ステップ、

・前記処理手段が、前記設定した鍵配布属性に基づいて前記暗号鍵を生成するか否かを判断し、前記判断の結果に基づいて前記暗号鍵を生成し、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能な鍵配布ステップ。

【０００８】

チャットシステムを例に取り説明する。例えば、チャットクライアントは、利用者情報としてニックネーム、ユーザＩＤ、チャネルオペレータか否か等を取得可能である。そこで、鍵配布属性を、例えばチャネルオペレータ属性に連動させ、チャネルオペレータであれば鍵配布属性ありに設定する。チャネル開設者により最初のチャネル暗号鍵を生成する。次にチャネルに参加してきたユーザは、チャネル開設者に対してチャネル暗号鍵を要求する。チャネル開設者は、前記要求に応じてチャネル暗号鍵を付与する。このように、ユーザ端末間でチャネル暗号鍵を配布し、サーバやボット上でのチャネル暗号鍵の解読を防止する。

【０００９】

本願第２発明は、他の通信装置と互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置とともに用いられ、記憶手段と、暗号化手段と、復号化手段と、利用者管理手段と、鍵取得手段と、鍵配布手段とを備えるセキュリティ強化装置を提供する。

記憶手段は、前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する。暗号化手段は、通信内容を前記通信装置から取得し、前記暗号鍵を用いて暗号化する。復号化手段は、通信内容を前記通信装置から取得し、前記暗号鍵を用いて復号化する。

【００１０】

利用者管理手段は、前記通信装置が前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を前記通信装置から取得し、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を、前記取得した利用者情報に基づいて設定し、取得した利用者情報及び設定した鍵配布属性を前記記憶手段に格納する。鍵取得手段は、前記設定した鍵配布属性に基づいて前記暗号鍵を取得するか否かを判断し、前記判断の結果に基づいて前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する。鍵配布手段は、前記設定した鍵配布属性に基づいて前記暗号鍵を生成するか否かを判断し、前記判断の結果に基づいて前記暗号鍵を生成し、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能である。

【００１１】

セキュリティ強化装置をチャットクライアントと共に用いる場合を例に取る。利用者管理手段は、チャネルに入るとそのチャネルに参加しているニックネームリストを含む利用者情報を、チャットクライアントを介して取得する。例えば、チャットクライアントは、利用者情報としてニックネーム、ユーザＩＤ、チャネルオペレータか否か等を取得可能である。そこで、鍵配布属性を、例えばチャネルオペレータ属性に連動させ、チャネルオペレータであれば鍵配布属性ありに設定する。次に、鍵取得手段は、ニックネームリストから鍵配布属性を有するいずれかの他の利用者を選択し、その利用者端末にチャネル暗号鍵を要求する。この要求を受け取った他の利用者端末では、鍵配布手段が、記憶手段からチャネル暗号鍵を取り出し、要求元の利用者端末に送信する。要求元の利用者端末は、鍵取得手段によりチャネル暗号鍵を受け取って記憶手段に格納する。暗号化手段及び復号化手段は、前記のようにして記憶手段に格納されたチャネル暗号鍵を用い、以降の会話内容を暗号化及び復号化する。

【００１２】

本願第３発明は、前記第２発明において、前記通信装置が、前記セキュリティ強化装置との連携手段を有している。さらに、連携手段は、前記暗号鍵の要求、前記要求に応じて送信される暗号鍵、前記利用者情報に関する情報及び所定の条件に合致する場合は通信内容の受け渡しを、通信装置とセキュリティ強化装置との間で行うセキュリティ強化装置を提供する。

【００１３】

例えば、受信した通信内容が暗号化されている場合、連携手段は、暗号化されている通信内容をセキュリティ強化装置に送出する。復号化された通信内容は連携手段を介してセキュリティ装置から通信装置に送出され、通常の会話内容と同様に表示される。逆に、通信内容を暗号化する場合、連携手段は入力された通信内容をセキュリティ強化装置に送出する。暗号化された通信内容は連携手段を介してセキュリティ強化装置から通信装置に送出され、通信装置により通常の会話内容と同様の扱いで送信される。

【００１４】

本願第４発明は、前記第２発明において、前記利用者管理手段が、所定の条件に基づいて、他の通信装置を選択し、前記暗号鍵の配布を許可する鍵配布属性を前記他の通信装置に付与するセキュリティ強化装置を提供する。さらに利用者管理手段は、鍵配布属性の設定及び設定対象の通信装置を前記通信装置から取得し、前記記憶手段に格納する。

【００１５】

たとえば、利用者管理手段は、そのチャットクライアントがチャネル開設者である場合に、他の利用者端末を選択する。選択方法は、チャネルに参加しているチャットクライアントからランダムに一定数選択したり、所定の参加順位までのチャットクライアントを選択するなどが挙げられる。他の利用者端末に鍵配布属性を付与可能にするために、具体的にはチャットシステムのプロトコルに新たに拡張プロトコルを設け、鍵配布属性を利用者情報として設定可能にすると良い。また、チャネルオペレータの設定と同様に、設定コマンドに基づいて鍵配布属性を付与可能にしても良い。

【００１６】
本願第５発明は、前記第２発明において、利用者管理手段が、他の通信装置の選択と、前記暗号鍵の配布を許可する鍵配布属性の前記他の通信装置への付与及び解除の指示とを受け付け、かつ鍵配布属性の設定及び設定対象の通信装置を前記通信装置から取得し、前記記憶手段に格納するセキュリティ強化装置を提供する。
【００１７】
利用者による鍵配布属性の設定及び解除を受け付け、個々の利用者端末にかかる鍵配布負担を利用者自身により調節可能にする。
本願第６発明は、前記第２発明において、鍵取得手段が所定の条件に基づいて前記暗号鍵の要求先を選択するセキュリティ強化装置を提供する。
すなわち、鍵取得手段は、乱数を発生させたり、鍵配布属性を有する通信装置から選択する等、所定の条件に基づいてチャネル暗号鍵の要求先を選択する。
【００１８】
本願第７発明は、前記第２発明において鍵取得手段が、所定の条件に基づいて前記暗号鍵の要求先を選択して前記暗号鍵を要求し、所定時間内に前記要求先から暗号鍵が送信されない場合、他の通信装置を選択して再度要求を行うセキュリティ強化装置を提供する。
要求先から一定時間内に暗号鍵が送信されてこない場合、鍵取得手段は要求先に何らかのトラブルがあったとして要求先の通信装置を選択し直す。選択基準は、ランダム、鍵配布属性のある通信装置など所定の条件を満たすものを選択する。
【００１９】
本願第８発明は、前記第２発明において、鍵取得手段が、前記通信内容が暗号化されている場合に前記暗号鍵の取得要求を行うセキュリティ強化装置を提供する。
例えば、チャットシステムにおいて、チャネル内の通信内容の全てを暗号化する暗号化モードを設定可能にしておく。鍵取得手段は、参加したチャネルのモードをチャットクライアントから取得し、暗号化モードがオンである場合は暗号鍵の取得要求を行う。
【００２０】
本願第９発明は、前記第２発明において、前記復号化手段が、前記通信装置から受け取る通信内容を復号不可能と判断した場合、前記暗号鍵の要求を行うことを決定し、前記鍵取得手段が、前記復号化手段の決定に従い、前記暗号鍵の取得要求を行うセキュリティ強化装置を提供する。
会話単位で暗号化を設定可能にすることも考えられる。例えば、ＧＵＩ(Graphic User Interface)によりコマンドボタンを表示し、このコマンドボタンのオンオフにより会話毎に暗号化の設定やその解除を行う。暗号化が設定されている場合、暗号化手段は、暗号化された会話内容の先頭部分に、会話の暗号化を示す暗号化フラグを記述する。通信装置は、会話内容に送信コマンドを付加し、ネットワークに送出する。復号化手段は、暗号化された会話内容を受け取ったが暗号鍵がない場合や、保持されている暗号鍵では復号化できない場合、暗号鍵を要求する旨の判断をする。鍵取得手段は、復号化手段の判断に従い、暗号鍵の取得要求を行う。
【００２１】
本願第１０発明は、前記第２発明において、前記記憶手段が複数の暗号鍵と暗号鍵を特定する鍵識別情報とを対応付けて記憶し、前記暗号化手段が、前記通信内容の暗号化に用いられた暗号鍵を示す鍵識別情報と通信内容とを、前記通信装置を介してネットワークに送出可能であり、前記復号化手段が、前記鍵識別情報で特定される暗号鍵は前記記憶手段に保持されているか否かを判断し、前記鍵取得手段が、前記判断結果に従い、前記鍵識別情報を通知して前記暗号鍵の取得要求を行うセキュリティ強化装置を提供する。
【００２２】
会話毎に暗号化の設定及び解除が行われる場合に、復号化手段がその会話の暗号化に用いられたチャネル暗号鍵を有していないと判断すれば、鍵取得手段はその判断に従ってチャネル暗号鍵の取得要求を行う。その際には、鍵識別番号を通知することにより、どの暗号鍵を要求しているかを特定する。鍵識別番号としては、チャネル生成時からのシリアル

番号や、チャネル暗号鍵にハッシュ関数等の一方向関数をかけたものなどが挙げられる。

【００２３】

本願第１１発明は、前記第２発明において、前記鍵取得手段が、利用者の公開鍵暗号系の公開鍵を前記暗号鍵の要求とともに通知し、前記要求に応じて送信される暗号鍵を利用者の秘密鍵を用いて復号化し、前記鍵配布手段が、前記要求元の公開鍵暗号系の公開鍵を用いて暗号化した前記暗号鍵を配布するセキュリティ強化装置を提供する。

【００２４】

暗号鍵を要求する要求元の鍵取得手段は、利用者の公開鍵を通知して要求を行う。要求を受け取った通信装置の鍵配布手段は、公開鍵を用いて暗号鍵を暗号化し、送り返す。要求元では、鍵取得手段が利用者の秘密鍵を用いて復号化し、暗号鍵を取得する。

本願第１２発明は、前記第２発明において、前記鍵配布手段が、他の前記通信装置から前記暗号鍵の要求があった場合、前記要求を検証し、検証結果に基づいて前記記憶手段からいずれかの暗号鍵を読み出し、前記他の通信端末に配布可能であるセキュリティ強化装置を提供する。

【００２５】

チャネル暗号鍵の要求を受け取った他の利用者端末では、まず鍵配布手段が要求を検証する。正当な要求者であれば、鍵配布手段は、記憶手段からチャネル暗号鍵を取り出して要求元の利用者端末に送信する。前述の要求元公開鍵を用いる例では、鍵配布手段は、要求元の公開鍵が正当な公開鍵か否かを検証することが好ましい。例えば、認証局の電子署名がある公開鍵や、ＩＲＣサーバの電子署名が施された公開鍵、暗号鍵の要求を受けたユーザの電子署名がある公開鍵などを、正当な公開鍵と見なすことが挙げられる。

【００２６】

本願第１３発明は、前記第２発明において、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置を提供する。

すなわち、適当なタイミングで暗号鍵を更新することにより、暗号鍵の解読を防止してセキュリティを高める。適当なタイミングとは、例えば所定の時間間隔、所定の会話数または会話量を超過したとき、ネットワークの参加利用者数が所定数を超えたときや下回ったとき、話題が変化したとき、最後の会話から所定時間経過したとき、利用者が暗号鍵の変更を指示したときなど様々なタイミングが考えられる。また、前記タイミングが生じても、会話が続行している最中は変更した鍵の配布を待機し、会話がとぎれたタイミングで鍵を再配布することも考えられる。

【００２７】

本願第１４発明は、前記第２発明において、所定のタイミングで前記暗号鍵を更新し、前記更新した暗号鍵を直前の暗号鍵を用いて暗号化して他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置を提供する。

前記更新された暗号鍵をその更新前の暗号鍵を用いて暗号化することにより、更新された暗号鍵を配布する際の解読のおそれを防止する。

【００２８】

本願第１５発明は、前記第２発明において、前記鍵変更手段が、前記各通信装置内に保持される秘密情報、時間情報及びネットワークに固有の情報のいずれかまたは全ての組合せに基づいて前記暗号鍵を生成するセキュリティ強化装置を提供する。

例えば、通信装置内に記憶されている基板番号やプログラムの格納アドレス、暗号鍵を更新する時間、チャネル名及びチャネルパスワードに基づいて、新たな暗号鍵を生成することが考えられる。

【００２９】

本願第１６発明は、前記第２発明において、前記鍵変更手段が、前記各通信装置内に保持される秘密情報、時間情報及びネットワークに固有の情報のいずれかの組合せまたは全てを、一方向関数で暗号化して前記暗号鍵を生成するセキュリティ強化装置を提供する。

例えば、通信装置内に記憶されている基板番号やプログラムの格納アドレス、暗号鍵を生成する時間、チャネル名及びチャネルパスワードを、ハッシュ関数で暗号化して暗号鍵

とする。

【００３０】

本願第１７発明は、前記第２発明において、前記利用者管理手段が、前記暗号鍵の更新及び配布を許可する鍵変更属性を、前記取得した利用者情報に基づいて設定して前記記憶手段に格納し、前記鍵変更属性の有無に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置を提供する。

【００３１】

前記鍵配布属性と同様、鍵変更属性をチャネルオペレータ属性に連動させて設定したり、チャネルに最後まで参加している利用者に設定してもよい。また、新たに拡張プロトコルを設けてチャットシステム上で鍵変更属性を設定可能にし、鍵変更属性を利用者情報として取得するようにしても良い。さらに、チャネルオペレータからの設定コマンドに基づいて鍵変更属性を設定することも可能である。

【００３２】

本願第１８発明は、前記第２発明において、前記利用者管理手段が、利用者が前記暗号鍵の更新及び配布を許可する鍵変更属性を有する場合に、所定の条件に基づいて他の通信装置を選択し、前記選択した通信装置に前記鍵変更属性を設定可能である。かつ、利用者管理手段は、鍵変更属性の設定及び設定対象の通信装置を前記通信装置から取得して前記記憶手段に格納する。さらに、前記鍵変更属性の有無に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置である。

【００３３】

鍵変更属性を有する利用者は、他の利用者に対して鍵変更属性を付与可能にしても良い。他の利用者の選択方法は、ランダムに一定数の通信装置を選択したり、チャネルへの参加順序に応じて一定数の通信装置を選択したり、任意の通信装置を通信装置リストから選択したり、様々である。鍵変更属性の設定は、例えばチャットシステム上で新たなコマンドを設定することにより可能になる。この設定に応じて、チャネルに参加しているユーザ端末は、ユーザ情報の書き換えをそれぞれ行う。

【００３４】

本願第１９発明は、前記第２発明において、前記利用者管理手段が、前記暗号鍵の更新及び配布を許可する鍵変更属性及び優先順位を、前記取得した利用者情報に基づいて設定して前記記憶手段に格納し、前記利用者情報の変化に従って前記優先順位の書き換えを行う。さらに、鍵変更属性及び優先順位に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えるセキュリティ強化装置である。

【００３５】

例えば、チャネルオペレータ属性に基づいて鍵変更属性を、チャネルへの参加順序に基づいて優先順位を設定する。第２位以降の利用者管理手段は、第１位の通信装置がネットワークから退出した場合や、前回の暗号鍵の更新から所定時間が経過して第１位の通信装置に何らかのトラブルがあったと判断する場合、利用者情報に基づいて自動的に優先順位をひとつづつ繰り上げる。新たな鍵の生成は、第１位のユーザが、所定のタイミングで行う。

【００３６】

本願第２０発明は、前記第２発明において、前記利用者管理手段が、利用者が前記暗号鍵の更新及び配布を許可する鍵変更属性を有する場合に、所定の条件に基づいて他の通信装置を選択し、前記他の通信装置に前記鍵変更属性と優先順位とを設定可能である。かつ、利用者管理手段は、鍵変更属性と優先順位との設定及び設定対象の通信装置を前記通信装置から取得して前記記憶手段に格納し、前記利用者情報の変化に従って前記優先順位の書き換えを行う。さらに、このセキュリティ強化装置は、前記鍵変更属性及び優先順位に基づいて、所定のタイミングで前記暗号鍵を更新し、他の通信装置に配布する鍵変更手段をさらに備えている。

【００３７】
例えば、チャネル暗号鍵の変更及び配布は、第１位の通信装置が行う。第２位以下の通信装置は、第１位の通信装置が配布する新たなチャネル暗号鍵を取得する。第２位以降の利用者管理手段は、第１位の通信装置がネットワークから退出した場合や、前回の暗号鍵の更新から所定時間が経過して第１位の通信装置に何らかのトラブルがあったと判断する場合、利用者情報に基づいて自動的に優先順位をひとつづつ繰り上げる。新たに第１位となった通信装置は、自ら暗号鍵の変更及び配布を行う。
【００３８】
本願第２１発明は、互いに同一のネットワークを共有して同時に双方向通信が可能な複数の通信装置から構成され、前記各通信装置が、記憶手段と、暗号化手段と、復号化手段と、利用者管理手段と、鍵取得手段と、鍵配布手段とを備えるセキュリティ強化システムを提供する。
記憶手段は、前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を保持する。
【００３９】
暗号化手段は、通信内容を前記暗号鍵を用いて暗号化する。復号化手段は、通信内容を前記暗号鍵を用いて復号化する。利用者管理手段は、前記いずれかのネットワークに参加している場合に、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を取得し、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を、前記取得した利用者情報に基づいて設定し、取得した利用者情報及び設定した鍵配布属性を前記記憶手段に格納する。
【００４０】
鍵取得手段は、前記設定した鍵配布属性に基づいて前記暗号鍵を取得するか否かを判断し、前記判断の結果に基づいて前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する。鍵配布手段は、前記設定した鍵配布属性に基づいて前記暗号鍵を生成するか否かを判断し、前記判断の結果に基づいて前記暗号鍵を生成し、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能である。
【００４１】
前記第２発明と同様の作用効果を有する。
本願第２２発明は、互いに同一のネットワークを共有して同時に双方向通信が可能な通信装置に用いられる、セキュリティ強化プログラムを記録したコンピュータ読み取り可能な記録媒体であって、下記Ａ～Ｆ段階を実行させるためのセキュリティ強化プログラムを記録した、コンピュータ読み取り可能な記録媒体を提供する。
・前記通信装置の処理手段が、前記共有されたネットワーク内の通信内容を暗号化及び復号化するための暗号鍵を記憶手段に保持する記憶段階、
・前記処理手段が、通信内容を前記通信装置から取得し、前記暗号鍵を用いて暗号化する暗号化段階、
・前記処理手段が、通信内容を前記通信装置から取得し、前記暗号鍵を用いて復号化する復号化段階、
・前記通信装置が前記いずれかのネットワークに参加している場合に、前記処理手段が、少なくとも前記ネットワークを共有する他の通信装置リストを含む所定の利用者情報を前記通信装置から取得し、他のセキュリティ強化装置に暗号鍵の配布を許可する鍵配布属性を前記取得した利用者情報に基づいて設定し、取得した利用者情報及び設定した鍵配布属性を前記記憶手段に格納する利用者管理段階、
・前記処理手段が、前記設定した鍵配布属性に基づいて前記暗号鍵を取得するか否かを判断し、前記判断の結果に基づいて前記他の通信装置リストからいずれかの通信装置を選択して前記暗号鍵を要求し、前記要求に応じて前記他の通信端末から送信される暗号鍵を前記記憶手段に格納する鍵取得段階、

・前記処理手段が、前記設定した鍵配布属性に基づいて前記暗号鍵を生成するか否かを判断し、前記判断の結果に基づいて前記暗号鍵を生成し、他の前記通信装置から前記暗号鍵の要求があった場合、前記記憶手段からいずれかの暗号鍵を読み出して前記他の通信端末に配布可能な鍵配布段階。

【００４２】

前記第２発明と同様の作用効果を有する。

【００４３】

【発明の実施の形態】

次に、本発明のセキュリティ強化装置について、実施形態例を挙げて具体的に説明する。以下の実施形態例においては、チャットシステムにおける会話内容のセキュリティを高めるために、本発明のセキュリティ強化装置をチャットクライアントとともに用いる場合を例に取り、説明する。

【００４４】

＜第１実施形態例＞

図１に、チャットクライアントと共に用いられるセキュリティ強化装置の機能構成図を示す。図１において、複数のユーザ端末Ａ，Ｂ，Ｃ，Ｄ，Ｅ…は、チャットクライアントが動作可能であり、チャットサーバとコンピュータネットワークを介して接続されている。セキュリティ強化装置１は、チャットクライアントとともに、各ユーザ端末に設けられている。

【００４５】

セキュリティ強化装置１は、記憶部２、ユーザ管理部３、鍵取得部４、鍵配布部５、鍵変更部６、鍵生成部７及び暗号化／復号化部８を有している。チャットクライアント１０には、セキュリティ強化装置１に応じ、ユーザＤＢ９、連携部１１及び振り分け部１２が設けられている。本実施形態例においては、セキュリティ強化装置１及びチャットクライアント１０を有する複数のユーザ端末Ａ～Ｅ間において、会話を暗号化／復号化するためのチャネル暗号鍵を生成し、配布する。

【００４６】

［セキュリティ強化装置］

記憶部２は、ユーザ自身の公開鍵系秘密鍵及び公開鍵を記憶している。また、記憶部２は、チャットクライアントが参加しているチャネルにおける会話を暗号化／復号化するためのチャネル暗号鍵を、鍵取得部４から受け取り、保持する。さらに、記憶部２は、チャネル暗号鍵を特定する暗号鍵ＩＤを鍵取得部４から受け取り、チャネル暗号鍵と暗号鍵ＩＤとを対応付けて暗号鍵リストに保持する。記憶部２に保持されるチャネル暗号鍵は、１つとは限らず複数でも良い。複数のチャネル暗号鍵が保持される場合には、記憶部２に保持するチャネル暗号鍵の最大数を予め設定またはユーザにより設定可能にしておくと良い。

【００４７】

ユーザ管理部３は、チャットクライアントがチャットサーバから取得するユーザ情報を参照し、参照したユーザ情報に基づいて、鍵配布属性及び鍵変更属性を設定する。図２に、鍵配布属性及び鍵変更属性を含めたユーザ情報の一例を示す。ここで、鍵配布属性とは、チャネル暗号鍵を他のユーザ端末に配布することが許可されていることを示す。また、鍵変更属性とは、チャネル暗号鍵を新たに更新し、他のユーザ端末に配布することが許可されていることを示す。

【００４８】

通常、チャットクライアントは、チャネルに参加することにより所定のユーザ情報をサーバから取得可能である。取得可能なユーザ情報としては、(1)ニックネーム、(2)ユーザの実際の氏名であるReal Name、(3)ネットワーク上でユーザを特定するためのユーザＩＤ、(4)チャットクライアントが動作している利用者端末を特定するクライアント名、(5)利用者端末が接続しているサーバを特定するサーバ名、(6)各ユーザが接続しているチャネルのリスト、(7)最終発言からの経過時間、(8)チャネルオペレータ属性の有無(0/1)など

が挙げられる。このうち、少なくともニックネームは、チャネル内のユーザを特定するために必要な情報である。

【００４９】

図２に示したユーザ情報の例では、チャットクライアントは、前記(1)～(8)のユーザ情報をチャットサーバから取得してユーザＤＢに書き込む。ユーザ管理部３は、チャットクライアントが取得したユーザ情報の中のチャネルオペレータ属性に基づいて鍵配布属性及び鍵変更属性を設定し、ユーザＤＢ９に書き込んでいる。チャネルオペレータ属性が"１"であれば、鍵配布属性及び鍵変更属性もそれぞれ"１"に設定される。また、ユーザ管理部３は、ユーザ情報の変化、例えば新たなチャネルオペレータの設定やユーザの退出を、後述するチャットクライアントの連携部１１を介して通知され、変化に応じてユーザ情報を更新する。

【００５０】

鍵配布属性や鍵変更属性の設定方法は、他にも考えられる。属性の他の設定方法として、ユーザ管理部３により所定の条件に基づいてユーザを選択し、選択したユーザに属性を設定する方法があげられる。鍵配布属性の付与対象の選択方法としては、例えば、乱数を発生させることによりランダムに一定数のユーザを選択したり、チャネルへの所定の参加順位までのユーザを手動であるいは自動的に選択したり、ユーザによる他のユーザの指定を受け付けることにより選択することが挙げられる。

【００５１】

鍵変更属性の付与対象の選択方法としては、例えば、チャネルの開設者を選択したり、チャネルに最後まで参加していたユーザを選択したりすることが挙げられる。また、鍵変更属性を有するユーザにより、例えば、チャネルへの参加順序に応じて一定数のユーザを選択したり、ランダムに一定数のユーザを選択したり、ユーザの手動による他のユーザの指定を受け付けて選択することが挙げられる。

【００５２】

これら選択したユーザに対し、属性を設定する方法の一つとして、属性配布コマンドを新たに設けることが考えられる。例えば、鍵配布属性の設定コマンドを"MODE #CH1 +d userA"、鍵変更属性の設定コマンドを"MODE #CH1 +x userA"とする。但し、ここで#CH1は任意のチャネル名、userAは任意のチャネル内ユーザのニックネームとする。ユーザ管理部３により、選択されたユーザ及び配布する属性を指定して前記コマンドをチャットクライアントに送出することにより、チャネルに参加している全ユーザ端末に前記コマンドが通知される。他のユーザ端末では、チャットクライアントを介してコマンドを受け取ったユーザ管理部３が、コマンドを解釈してユーザ情報の書き換えを行う。

【００５３】

複数のユーザが鍵変更属性を有する場合、ユーザ管理部３によりチャネル暗号鍵を変更する優先順位を併せて設定することが好ましい。例えば、チャネルオペレータ属性に連動させて鍵変更属性を設定する場合は、チャネル開設者の優先順位を第１位とし、他のユーザの優先順位はチャネルに参加した順に設定する。また、鍵変更属性を有するユーザが一人であり、そのユーザから他のユーザに鍵変更属性を付与する場合は、最初に鍵変更属性を有していたユーザの優先順位を第１位とする。そして、ユーザ管理部３により選択されるユーザに対し、チャネルへの参加順序に応じて、ランダムに、または手動による指定を受け付け、優先順位を設定する。

【００５４】

前記優先順位を設定するために、前記属性設定コマンドにより属性と共に優先順位の設定も可能にしておくことが好ましい。例えば、鍵変更属性の設定コマンドにおいて、拡張子"+x"のあとに優先順位を示す自然数"n"を記述することにより、優先順位を設定することが考えられる。例えば、"userA"に第２位の鍵変更属性を設定するコマンドは、"MODE #CH1 +x2 userA"となる。鍵変更属性と共に設定される優先順位は、チャネル内の全てのユーザ端末に通知される。従って、各ユーザ端末のユーザ管理部３は、ユーザ情報の変化、例えばいずれかのユーザが退出することにより鍵変更属性の優先順位に変更が生じると、

生じた変化に応じて優先順位を書き換えることが出来る。

【００５５】

鍵取得部４は、所定の条件に基づいて、他のユーザの選択及び選択したユーザへのチャネル暗号鍵の要求を行う。また、要求に応じて送信されてくるチャネル暗号鍵を記憶部２に格納する。チャネル暗号鍵の要求先の選択方法は特に限定されない。例えば、乱数を発生させることによりランダムに一意のユーザを選択したり、鍵配布属性を有するユーザからチャネルに参加した順に選択することが挙げられる。選択したユーザ端末が多忙であったり、通信路が混雑しているなど、何らかの事情により選択したユーザ端末から一定時間経過しても応答がない場合、鍵取得部４は、他のユーザ端末を選択し、再びチャネル暗号鍵の要求を行う。

【００５６】

チャネル暗号鍵の要求は、所定の情報及びユーザ証明書を送信することにより行う。所定の情報とは、チャネル名と、ニックネームなどの要求元ユーザを特定する情報とを最低限含んでいる。ユーザ証明書は、ユーザに関する情報、すなわち証明書本体と、要求元ユーザの公開鍵と、証明者である認証局の電子署名とから構成されている。証明者としては、認証局が一般的ではあるが、他にユーザ端末が接続するサーバや、鍵を要求する先のユーザなどでも良い。

【００５７】

前記チャネル暗号鍵の要求を行うタイミングは、鍵取得部４が通信の暗号化を確認したときである。具体的には、そのチャネル内の通信が全て暗号化されている暗号化モードを確認したとき、または暗号化された会話を受信したときである。前者の場合、チャネル内の全会話を暗号化する暗号化モードの設定コマンドを予め準備しておく。例えば、"MODE #CH1 +c"などのように、"MODE"コマンドの拡張子を用いたコマンドを準備する。通常、チャットクライアントがチャネルに参加すると、そのチャネルに設定されているモードが通知される。鍵取得部４は、このモードをチャットクライアントの連携部１１から取得し、暗号化モードであればチャネル暗号鍵の要求を行う。

【００５８】

後者の場合、会話毎にその会話が暗号化されているか否かを示す暗号化フラグを、各会話と共に送信することが考えられる。通常のチャットシステムにおいては、会話を送信する送信コマンドと会話内容とからなる会話メッセージが作成される。本実施形態例においては、さらに暗号化のオン／オフを示す暗号化フラグ（０／１）を会話内容の先頭部分に記述して会話メッセージを作成する。

【００５９】

また、暗号化フラグに代えて暗号鍵ＩＤを用いることも考えられる。暗号化フラグを会話内容に記述することは、後述するように暗号化／復号化部８が行う。鍵取得部４は、暗号化／復号化部８がチャットクライアントから受け取る会話内容を復号化できない場合、後述する暗号化／復号化部８の指示に従ってチャネル暗号鍵の要求を行う。暗号化／復号化部８が復号化を行えない場合については後述する。

【００６０】

鍵取得部４は、要求元ユーザの公開鍵で暗号化されたチャネル暗号鍵を受信し、これをユーザの秘密鍵で復号化してチャネル暗号鍵を取得する。また、暗号化されたチャネル暗号鍵と共に暗号鍵ＩＤを受信し、取得したチャネル暗号鍵と暗号鍵ＩＤとを記憶部２の暗号鍵リストに格納する。

さらに、鍵取得部４は、ユーザ端末に鍵変更属性がない場合か、鍵変更属性を有していても優先順位が第１位でない場合には、他のユーザ端末から送信される新たなチャネル暗号鍵を取得する。取得した新たなチャネル暗号鍵は直前のチャネル暗号鍵を用いて暗号化されているので、鍵取得部４は、直前のチャネル暗号鍵を記憶部２から取り出し、送信されてきたチャネル暗号鍵を復号化する。また、前記と同様に、復号化したチャネル暗号鍵から暗号鍵ＩＤを求め、チャネル暗号鍵と対応付けて暗号鍵リストに格納する。さらに、鍵取得部４は、チャネル暗号鍵が更新される所定のタイミングを経過しても新たなチャネ

ル暗号鍵を受信しない場合、ユーザ管理部３に対して優先順位の変更の指示を通知する。この通知を受け、ユーザ管理部３により鍵変更属性の優先順位の繰り上げが行われる。チャネル暗号鍵の更新については後述する。

【００６１】

鍵配布部５は、他のユーザ端末から送信されるチャネル暗号鍵の要求を検証する。要求の検証には、チャネル暗号鍵の要求とともに要求元から送信されるユーザ証明書を用いる。検証の結果、要求元が正当なユーザであることを判断すると、最新のチャネル暗号鍵を暗号鍵リストから取り出し、ユーザ証明書に含まれる要求元の公開鍵で暗号化する。鍵配布部５は、前記取り出したチャネル暗号鍵にハッシュ関数などの一方向関数をかけて暗号鍵ＩＤを求め、暗号化したチャネル暗号鍵と暗号鍵ＩＤとを要求元に送信する。暗号鍵ＩＤはチャネル暗号鍵を一義的に特定できればよいので、シリアル番号やチャネル暗号鍵を生成した日付及び時刻などを暗号鍵ＩＤとして用いても良い。また、鍵配布部５は、要求とともに暗号鍵ＩＤが送信された場合は、暗号鍵ＩＤにより指定されるチャネル暗号鍵を送信する。

【００６２】

鍵変更部６は、適当なタイミングでチャネル暗号鍵を新たに生成し、生成したチャネル暗号鍵を他のユーザ端末に送信する。新たにチャネル暗号鍵を生成するタイミングとしては、例えば一定時間経過毎に生成することが挙げられる。また、チャットクライアントにおける会話数や会話のデータ量を監視することにより、ある一定会話数毎に、あるいは一定会話量毎に生成してもよい。さらに、ユーザ情報を監視して、チャネル内ユーザ数が所定数、例えば１になったとき、チャネルのトピックが変化したとき、最後の会話から所定時間経過したとき、ユーザがチャネル暗号鍵の変更を指示する任意の時など、様々なタイミングが考えられる。鍵変更部６は、生成したチャネル暗号鍵をすぐに送信しても良いが、会話が断続的に続いているような状態では送信を見合わせ、会話がとぎれたときに送信を行うようにすると好ましい。

【００６３】

新たなチャネル暗号鍵の生成は、例えばユーザ端末内に保持されている秘密情報、時間情報、チャネル固有情報などの情報を組み合わせ、ハッシュ関数などの一方向関数をかけることにより生成するとよい。ユーザ端末内に保持されている秘密情報とは、端末内の基板の製造番号や、ある特定のプログラムのアドレスなど、第３者が容易に想到しにくい情報が好ましく、さらに時間的に静的情報ではなく変化する情報であればさらに好ましい。

【００６４】

時間情報としては、前記チャネル暗号鍵の生成タイミングにおける時刻データを、時刻データ取得プログラムルーチンを用いて取得する。時刻データ取得プログラムルーチンは、ユーザ端末の内部時計を利用しており、通常ユーザ端末上で動作するオペレーティングシステムにより提供されている。時刻データとしては、時刻データ取得プログラムルーチンが出力する1970年1月1日からの通算秒が一般に用いられる。チャネル固有情報としては、例えばチャネル名やチャネルに設定されているパスワードなどが挙げられる。

【００６５】

生成した新たなチャネル暗号鍵は、そのまま送信するよりも、暗号化して送信する方がセキュリティの観点から好ましい。例えば、１つ前のチャネル暗号鍵を用いて新たなチャネル暗号鍵を暗号化して送信すると、受信側も復号可能である上に盗聴を防止しやすいと考えられる。

前記チャネル暗号鍵の生成及び配布は、ユーザ情報の鍵変更属性に基づいて行うことが好ましい。すなわち、ユーザ情報の鍵変更属性が付与されている場合のみ、前記チャネル暗号鍵を生成し、配布する。鍵変更属性は、前述のように各ユーザ端末においてユーザ管理部３により設定される。鍵変更属性とともに優先順位が設定されている場合は、例えば次のようにしてチャネル暗号鍵の更新を行う。

【００６６】

優先順位が第１位のユーザにおいては、鍵変更部６は前述のように所定のタイミングで

新たなチャネル暗号鍵を生成し、他のユーザ端末に送信する。優先順位が第２位以降のユーザにおいては、所定時間経過しても新たなチャネル暗号鍵が送信されてこない場合、第１位のユーザ端末が何らかの事情でチャネル暗号鍵を送信できなかったものと判断する。この判断は、前述のように鍵取得部４で行う。そして、ユーザ管理部３により順次優先順位の繰り上げが行われた結果新たに第１位となったユーザが、チャネル暗号鍵の生成及び配布を行う。

【００６７】

鍵生成部７は、チャットクライアントがチャネル開設者である場合、最初のチャネル暗号鍵を生成する。生成方法は、前記チャネル暗号鍵の更新と同様に、ユーザ端末内の秘密情報、時間情報、チャネル固有情報などの情報を組み合わせ、ハッシュ関数をかけて生成するとよい。時間情報としては、例えばチャネルを開設した時刻のデータを用いるなどが考えられる。また、鍵生成部７は、生成したチャネル暗号鍵にハッシュ関数をかけるなどして前述の鍵配布部５と同様に暗号鍵ＩＤを作成し、チャネル暗号鍵と暗号鍵ＩＤとを対応付けて記憶部２に格納する。

【００６８】

暗号化／復号化部８は、後述するチャットクライアントの振り分け部１２から暗号化された会話内容が送出されることに従い、記憶部２に保持されているチャネル暗号鍵を取り出し、会話内容の復号化を行う。復号化に用いるチャネル暗号鍵には通常は最新のチャネル暗号鍵を用いるが、会話内容の先頭に暗号鍵ＩＤが記述されている場合、暗号鍵ＩＤにより特定されるチャネル暗号鍵を用いて復号化を行う。

【００６９】

また、暗号化／復号化部８は、復号化を行うことができない場合、鍵取得部４に対し鍵要求を行うことを指示する。復号化を行うことができない場合とは、(1)記憶部２にチャネル暗号鍵が保持されていない場合または(2)通知された暗号鍵ＩＤに対応するチャネル暗号鍵が記憶部２に保持されていない場合である。復号化した会話内容は、再びチャットクライアントに送出され、通常のメッセージを受信した場合と同様に画面上に表示される。

【００７０】

さらに、暗号化／復号化部８は、振り分け部１２から会話内容を受け取ると、最新のチャネル暗号鍵を用いて暗号化する。ついで、暗号化した会話内容の先頭部分に暗号化フラグまたは暗号鍵ＩＤを記述し、再びチャットクライアントに送出する。チャットクライアントでは、通常の会話内容と同様に、セキュリティ強化装置１から送出されたデータに送信コマンドを付加し、送信する。

【００７１】

［チャットクライアント］

図１に示すように、本実施形態例におけるチャットクライアント１０には、連携部１１と振り分け部１２とがセキュリティ強化装置１に応じて設けられている。連携部１１は、チャットクライアントが送受信するコマンドを解釈し、セキュリティ強化装置１の各構成要素に処理を振り分ける。具体的には、連携部１１は、ユーザ情報が変化するコマンドを解釈すると、ユーザ情報の変化及びその内容をユーザ管理部３にユーザ管理部３に通知する。前記コマンドとしては、例えばユーザの退出を示すコマンド"PART"、参加を示すコマンド"JOIN"、チャネルオペレータの特権を授与するコマンド"MODE #CH1 +o"、鍵配布属性の設定コマンド"MODE #CH1 +d userA"、鍵変更属性及び優先順位の設定コマンド"MODE #CH1 +xn userA"等が挙げられる。また、逆に、ユーザ管理部３からの鍵配布属性の設定コマンド"MODE #CH1 +d userA"、鍵変更属性及び優先順位の設定コマンド"MODE #CH1 +xn userA"等を受け付け、処理する。

【００７２】

連携部１１は、チャネル暗号鍵の授与を示すコマンドや暗号化モードの設定コマンドを解釈すると、鍵取得部４に対し通知する。また、鍵取得部４からチャネル暗号鍵の取得を要求するコマンドを受け付け、処理する。

連携部１１は、チャネル暗号鍵の要求を示すコマンドを解釈すると、鍵配布部５に対し要求を通知する。また、鍵配布部５からの要求に対してチャネル暗号鍵の授与コマンドを受け付け、処理する。

【００７３】

振り分け部１２は、送信されてきた会話メッセージの先頭部分が暗号化フラグ"１"または暗号鍵ＩＤである場合、復号化の指示を暗号化／復号化部８に通知する。具体的には、暗号化フラグまたは暗号鍵ＩＤと暗号化された会話内容とを暗号化／復号化部８に送出する。

また、振り分け部１２は、利用者からの暗号化の指示及び解除を受け付け、暗号化が指示されている場合には、入力された会話内容を暗号化／復号化部８に送出する。暗号化の指示及び解除は、例えばＧＵＩ(Graphic User Interface)を利用してコマンドボタンを画面上に表示させ、コマンドボタンのオン／オフによりなされるようにすることが出来る。さらに、振り分け部１２は、暗号化／復号化部８により暗号化され、暗号化フラグまたは暗号鍵ＩＤを含む会話内容を、通常の会話内容と同様に処理する。すなわち、暗号化された会話内容は、チャットクライアントにより通常の会話内容と同様に、送信コマンドを付加され、通常のチャットシステムにおける発言として送信される。

【００７４】

［処理の流れ］

次に、セキュリティ強化装置１が行う主な処理の流れを説明する。図３は、セキュリティ強化装置１が行うメインルーチンの処理の流れを示すフローチャートである。図４～６は、メインルーチンにおいて行われる処理の詳細を示している。図４は、他のユーザ端末から鍵を取得するための鍵取得処理の流れを示すフローチャート、図５は、他のユーザ端末に鍵を配布する鍵配布処理の流れを示すフローチャート、図６は、他のユーザからの鍵の要求を検証する要求検証処理の流れを示すフローチャートである。また、図７は、メインルーチンと独立に行われ、所定の条件に従ってチャネル暗号鍵を変更する場合の鍵変更処理の流れを示すフローチャートである。

【００７５】

（１）メインルーチン

ユーザ端末においてチャットクライアントがチャネルに参加またはチャネルを開設することにより、図３のメインルーチンの処理が開始される。説明を容易にするため、鍵配布属性及び鍵変更属性をチャネルオペレータに連動させて設定する場合を例に取り、説明する。

【００７６】

ステップＳ１では、ユーザ管理部３が、ユーザ情報のチャネルオペレータに連動させて、鍵配布属性及び鍵変更属性を設定する。

ステップＳ２では、ユーザ管理部３は、ユーザがチャネルの開設者か否かを判断する。チャネル内のユーザが１人だけ、すなわちチャネルに参加しているチャットクライアントが自己のチャットクライアントだけであれば、そのユーザはチャネル開設者であるのでステップＳ３に移行する。チャネルの開設者ではなく複数のユーザがチャネル内にいれば、チャネル暗号鍵を取得するためにステップＳ４に移行する。

【００７７】

ステップＳ３では、チャネル開設者のユーザ端末において、鍵生成部７がチャネル暗号鍵を生成する。さらに、生成したチャネル暗号鍵に暗号鍵ＩＤを付し、記憶部２の暗号鍵リストに格納し、ステップＳ５に移行する。

ステップＳ４では、チャネル開設者ではないユーザが、後述する鍵取得サブルーチンにより他のユーザ端末に対してチャネル暗号鍵の要求を行い、チャネル暗号鍵を取得する。

【００７８】

ステップＳ５では、後述する鍵配布サブルーチンにより、鍵配布属性を有するユーザが他のユーザ端末にチャネル暗号鍵を配布する。

ステップＳ６では、当該チャットクライアントがチャネルから退出するか否かを判断し

、退出するのであれば処理を終了する。退出しないのであれば、再びステップＳ５に戻り、他のユーザからの要求に応じてチャネル暗号鍵を配布する。

【００７９】

なお、図示していないが、ユーザ管理部３は、メインルーチンとは独立にチャットクライアントからのユーザ情報の変更の通知を受け付け、通知に従って鍵配布属性及び鍵変更属性をを更新している。

（２）鍵取得処理

次に、前記メインルーチンのステップＳ４で行う鍵取得処理について、図４を参照しながら説明する。

【００８０】

まず、ステップＳ１１では、鍵取得部４が、暗号化モードの設定になっているかどうかを判断する。暗号化モードであれば、会話内容は全て暗号化されており、チャネル暗号鍵を取得する必要があるので、後述するステップＳ１３に移行する。暗号化モードでなければステップＳ１２に移行する。

ステップＳ１２では、鍵取得部４は、暗号化／復号化部８から鍵の取得を指示されているか否かを判断する。チャネル暗号鍵を取得していない状態で暗号化フラグが"１"または暗号鍵ＩＤを含む会話メッセージを受信した場合、暗号化／復号化部８は鍵取得部４に対して鍵の取得を指示するからである。ステップＳ１２では、暗号化／復号化部８からの指示を待機し、指示があるとステップＳ１３に移行する。

【００８１】

ステップＳ１３では、鍵取得部４が、他のユーザを選択するための乱数を発生させる。

ステップＳ１４では、鍵取得部４が、発生させた乱数に基づいて、鍵配布属性を有する他のユーザの中からいずれかのユーザを選択する。

ステップＳ１５では、鍵取得部４が、記憶部２からユーザの公開鍵を取り出し、チャネル名及びニックネームにユーザの公開鍵を含むユーザ証明書を添付し、チャネル暗号鍵の要求を送信する。前述のように、鍵取得部４は、暗号鍵ＩＤを含む会話メッセージの受信に応じてチャネル暗号鍵を要求する場合には、暗号鍵ＩＤを指定して要求を送信する。逆に、暗号化モードの通知または暗号化フラグが“１”の会話メッセージの受信に応じて要求を行う場合には、暗号鍵ＩＤを指定せずに要求を送信する。

【００８２】

ステップＳ１６では、鍵取得部４が、チャネル暗号鍵及び暗号鍵ＩＤを受信したか否か判断し、まだであればステップＳ１７に移行する。受信していればステップＳ１８に移行する。

ステップＳ１７では、鍵取得部４が、所定時間Ｔが経過しているか否かを判断し、まだであればステップＳ１６に戻ってチャネル暗号鍵の受信を待機する。所定時間Ｔが経過していれば、鍵取得部４は、選択したユーザが何らかの理由によりチャネル暗号鍵を送信できないものと判断し、他のユーザ端末を再度選択すべくステップＳ１３に戻る。

【００８３】

ステップＳ１８では、鍵取得部４が、受信した暗号鍵をユーザの公開鍵を用いて復号化してチャネル暗号鍵を得、チャネル暗号鍵と共に受信した暗号鍵ＩＤとともに暗号鍵リストに格納し、処理を終了する。

（３）鍵配布処理

次に、前記メインルーチンのステップＳ５で行う鍵配布処理について、図５を参照しながら説明する。

【００８４】

まず、ステップＳ２１では、鍵配布部５が、ユーザ情報を参照し、自己のユーザ端末に鍵配布属性があるか否かを判断する。鍵配布属性がなければ処理を終了し、あればステップＳ２２に移行する。

ステップＳ２２では、鍵配布部５が、他のユーザ端末からのチャネル暗号鍵の要求を受け取ったか否かを判断する。受け取っていればステップＳ２３に移行し、受け取っていな

ければ、要求を受け取るまで待機する。

【００８５】

ステップＳ２３では、鍵配布部５が、後述する要求検証サブルーチンを実行し、要求の送信元が正当なユーザか否かを検証して検証結果を得る。

ステップＳ２４では、鍵配布部５が、検証結果に基づき要求元ユーザが正当なユーザか否かを判断し、正当でなければステップＳ２５に移行する。正当なユーザであれば、ステップＳ２６に移行する。

【００８６】

ステップＳ２５では、鍵配布部５が、正当でないユーザに対して例えばチャネル暗号鍵を配布できない旨のメッセージを送信するなどの適当な処理を行う。

ステップＳ２６では、要求元が正当なユーザであったので、鍵配布部５は、チャネル暗号鍵の要求とともに送られて来ているユーザ証明書から要求元ユーザの公開鍵を取り出す。

【００８７】

ステップＳ２７では、鍵配布部５が、最新のチャネル暗号鍵を暗号鍵リストから取り出す。要求と共に暗号鍵ＩＤが送信されてきている場合は、暗号鍵ＩＤにより特定されるチャネル暗号鍵を取り出す。また、取り出したチャネル暗号鍵にハッシュ関数をかけて暗号鍵ＩＤを求める。

ステップＳ２８では、鍵配布部５が、前記チャネル暗号鍵を要求元ユーザの公開鍵で暗号化する。

【００８８】

ステップＳ２９では、鍵配布部５が、暗号化されたチャネル暗号鍵及び暗号鍵ＩＤを、チャットクライアントを介して要求元ユーザ端末に送信し、メインルーチンに戻る。

（４）要求検証処理サブルーチン

次に、前記鍵配布サブルーチンのステップＳ２３で行う要求検証処理について、図６を参照しながら説明する。

【００８９】

ステップＳ３１では、鍵配布部５が、チャネル暗号鍵の要求とともに送信されてきたユーザ証明書を取り出す。

ステップＳ３２では、鍵配布部５が、ユーザ証明書の中の認証局の電子署名を取り出す。

ステップＳ３３では、鍵配布部５が、前記取り出した電子署名を、通常ユーザ端末が有する認証局データベースのなかから検索する。

【００９０】

ステップＳ３４では、鍵配布部５が、前記検索の結果に基づいて電子署名が認証局ＤＢに登録されているか否かを判断し、登録されていなければステップＳ３９１に移行する。登録されていればステップＳ３５に移行する。

ステップＳ３５では、鍵配布部５が認証局の公開鍵を認証局ＤＢから取得する。

【００９１】

ステップＳ３６では、鍵配布部５が、前記電子署名を認証局の公開鍵で復号化し、ユーザ証明書のメッセージダイジェスト（ＭＤ）を求める。

ステップＳ３７では、鍵配布部５が、前記ユーザ証明書のうち、前記電子署名の対象となっている部分を取り出し、通常用いられるアルゴリズムを用いてメッセージダイジェスト（ＭＤ'）を計算する。通常用いられるアルゴリズムとしては、例えばＭＤ５やＳＨＡなどが挙げられる。

【００９２】

ステップＳ３８では、鍵配布部５が、２つのメッセージダイジェストを比較し、両者が一致していればステップＳ３９に移行する。一致しなければステップＳ３９１に移行する。

ステップＳ３９では、鍵配布部５が「要求元ユーザは正当である」旨を検証結果とする

。

【００９３】

ステップＳ３９１では、鍵配布部５が、要求元ユーザを不当なユーザとして扱い、例えば要求元ユーザに不当である旨の通知を送出する。

（５）鍵変更処理

次に、前記メインルーチンと平行して独立に行われる鍵変更処理について、図７を参照しつつ説明する。

【００９４】

まず、ステップＳ４１では、鍵変更部６が、当該ユーザ端末に鍵変更属性があるか否かを、ユーザ情報を参照して判断する。鍵変更属性がないと判断すると、後述するステップＳ５０に移行する。鍵変更属性があると判断すると、ステップＳ４２に以降する。

ステップＳ４２では、鍵変更部６が、当該ユーザ端末に鍵変更属性とともに付与されている優先順位が第１位か否かを判断する。第１位であればステップＳ４３に移行し、第２位以降であれば後述するステップＳ５０に移行する。

【００９５】

ステップＳ４３では、鍵変更部６が所定のトリガの発生を待機し、所定のトリガが発生すると、ステップＳ４４に移行する。今、説明を分かりやすくするために、チャネル内ユーザが１人になったときまたは所定時間毎に、チャネル暗号鍵を変更するものとする。具体的には、チャネル内ユーザが最後の１人になった場合、またはチャネル内に複数のユーザがいても前回の変更から所定時間が経過している場合に、ステップＳ４４に移行する。

【００９６】

ステップＳ４４では、鍵変更部６が、予め決めておいた規則により暗号鍵を生成する。例えば、ユーザ端末において本プログラムが格納されているアドレス、前記トリガが発生した時刻、チャネル名及びチャネルのパスワードの組合わせにハッシュ関数をかけたものを新たなチャネル暗号鍵とする。また、新たなチャネル暗号鍵にハッシュ関数をかけて暗号鍵ＩＤを求める。

【００９７】

ステップＳ４５では、鍵変更部６が、直前のチャネル暗号鍵を暗号鍵リストから取得する。

ステップＳ４６では、鍵変更部６が、生成した新たな暗号鍵を直前のチャネル暗号鍵で暗号化する。

ステップＳ４７では、鍵変更部６が、暗号化した新たなチャネル暗号鍵の送信を行うか否かを、現在の会話状況に基づいて判断する。例えば、最後の発言から所定時間経過していれば、会話がとぎれていると判断してステップＳ４８に移行する。所定時間経過していなければ、会話が断続的に続いていると判断し、再度ステップＳ４７を繰り返して会話がとぎれるのを待機する。

【００９８】

ステップＳ４８では、鍵変更部６が、暗号化された新たなチャネル暗号鍵及び暗号鍵ＩＤを、チャットクライアントを介して他のユーザ端末に送信する。

ステップＳ４９では、当該ユーザ端末のチャットクライアントがチャネルから退出したか否かを判断し、退出していれば処理を終了する。退出していなければ、再びステップＳ４２に戻り、前記処理を繰り返す。

【００９９】

ステップＳ４１で鍵変更属性がないと判断された場合、または、ステップＳ４２で鍵変更属性の優先順位が第２位以下であると判断された場合、ステップＳ５０に移行して新たなチャネル暗号鍵の取得を行う。

ステップＳ５０では、鍵取得部４が、前回のチャネル暗号鍵の変更から所定時間経過するのを待機し、所定時間が経過するとステップＳ５１に移行する。本実施形態例においては、鍵取得部４は、ユーザ端末内の内部時計を参照することにより、前回のチャネル暗号鍵の変更からの経過時間を監視する。

【０１００】
ステップＳ５１では、鍵取得部４が新たなチャネル暗号鍵を取得したか否かを判断し、まだ取得していなければ鍵取得部４はユーザ管理部３に対して優先順位の繰り上げを通知し、ステップＳ５２に移行する。取得していれば後述するステップＳに移行する。
ステップＳ５２では、前記通知を受けたユーザ管理部３が、鍵変更属性の優先順位が第２位以降のユーザの優先順位を順次繰り上げ、ユーザ情報の書き換えを行う。これにより、書き換え前は第２位以降であったユーザ全ての優先順位が変化する。
【０１０１】
ステップＳ５３では、優先順位の書き換えにより優先順位が第１位になったか否かを鍵変更部６により判断し、第１位であればステップＳ４３に移行して前記チャネル暗号鍵の変更を行う。優先順位が第２位以降であれば、前記ステップＳ５０に移行し、新たなチャネル暗号鍵の取得を行う。
ステップＳ５４では、他のユーザ端末から送信された新たなチャネル暗号鍵を取得したので、鍵取得部４が、暗号化されたチャネル暗号鍵を直前のチャネル暗号鍵を用いて復号化し、新たなチャネル暗号鍵を得る。
【０１０２】
ステップＳ５５では、取得部が、得られたチャネル暗号鍵と暗号鍵ＩＤとを対応付けて暗号鍵リストに格納する。
ステップＳ５６では、当該ユーザ端末のチャットクライアントがチャネルから退出したか否かを判断し、退出していれば処理を終了する。退出していなければ、再びステップＳ４１に戻り、前記処理を繰り返す。
【０１０３】
＜第２実施形態例＞
チャットクライアント間で１対１の会話を行う場合は、会話の開始元の鍵取得部４が、相手先に対して自分の公開鍵を付加してセッション鍵要求を出す。
要求を受けた相手先では、鍵生成部７がセッション鍵を生成し、要求元の公開鍵でセッション鍵を暗号化して要求元に送る。セッション鍵は、前記第１実施形態例と同様、会話の開始元や相手先の固有情報、時刻、クライアントに内蔵される秘密情報の組合せに対し、ハッシュ関数をかけて生成すると良い。
【０１０４】
さらに、前記第１実施形態例と同様、新規セッション鍵は直前のセッション鍵を用いて暗号化して相手先に送ることが好ましい。また送信の際には、新規セッション鍵を相手先の公開鍵で暗号化して送信することが好ましいのも第１実施形態例と同様である。
要求元の鍵取得部４は、ユーザの秘密鍵でセッション鍵を復号化し、記憶部２に格納する。以降、相互にセッション鍵によってメッセージを暗号化して会話を行う。
【０１０５】
セッション鍵の変更のタイミングや条件は、前記第１実施形態例と同様である。すなわち、所定時間が経過したとき、所定会話数を超過したとき、所定会話量を超過したときなどにセッション鍵を変更する。また、セッション鍵の変更は、会話の開始元が行っても、また会話の相手先が行ってもよい。セッション鍵の変更を、前回メッセージを送信した方が行ったり、前回メッセージを受信した方が行ったりしてもよい。
【０１０６】
なお、会話開始の要求を受けた鍵配布部５が、要求に付加されている公開鍵の正当性をチェックし、不当な場合は要求を受け付けないことはいうまでもない。公開鍵は、通常利用者端末に内蔵されている認証局の電子署名が施された公開鍵や、接続中のサーバの電子署名が施された公開鍵や、自らが電子署名した公開鍵を正当として認めることが考えられる。
【０１０７】
＜第３実施形態例＞
前記の第１実施形態例においては、セキュリティ強化装置１に設けたユーザ管理部３に

より鍵配布属性及び鍵変更属性を設けたが、他の方法も可能である。例えば、チャネルオペレータ属性などと同様に、鍵配布属性及び鍵変更属性をチャットシステム上のユーザ属性として設ける。各チャットクライアントは、ニックネームやチャネルオペレータ属性などと同様に、鍵配布属性及び鍵変更属性をユーザ情報の一部としてチャットサーバから取得し、ユーザＤＢに格納する。セキュリティ強化装置は、ユーザＤＢ内のユーザ情報を参照し、前述の処理を行う。

【０１０８】

＜第４実施形態例＞

前記の第１実施形態例においては、チャネル暗号鍵を変更するタイミングを鍵取得部４により監視しているが、他の形態も考えられる。例えば、鍵生成部７、鍵配布部５及び鍵変更部６は、チャネル暗号鍵と共にチャネル暗号鍵が次に変更される時刻を送信する。各ユーザ端末は、チャネル暗号鍵と共にチャネル暗号鍵の有効期限を持つことになる。各ユーザ端末の鍵取得部４は、チャネル暗号鍵の有効期限をチャネル暗号鍵の変更タイミングとする。チャネル暗号鍵と共にチャネル暗号鍵の有効期限を示す時刻を送信することにより、チャネル暗号鍵の変更を所定時間毎に行うことはもちろん、任意のタイミングで行うことが出来る。

【０１０９】

もっとも、各ユーザ端末において内部時計にずれがある場合も考えられる。そこで、チャネル暗号鍵の有効期限を示す情報として、時刻に代えて相対時間及び起点時刻を用いることが考えられる。起点時刻としては、チャネル暗号鍵が生成された時刻を用い、相対時間としては、生成時刻を起点とした場合に次にチャネル鍵が変更されるまでの時間を用いる。

【０１１０】

また前述のように、時間に基づくのではなく他の変化が生じた場合、例えばチャネル内ユーザが一人になった場合にチャネル暗号鍵の変更を行うこともあり得る。このような設定では、変化の頻度が少なすぎ、チャネル暗号鍵が長時間変更されない場合も考えられる。このような場合を防止する方法として、例えば次のような方法が挙げられる。

【０１１１】

通常、鍵の生成に用いられるアルゴリズムは、鍵に有効期限を持たせている。そこで、鍵生成部７、鍵配布部５及び鍵変更部６により、チャネル暗号鍵と共にその有効期限を各ユーザ端末に送信する。鍵取得部４は、チャネル暗号鍵の有効期限まで所定の変化が生じなかった場合、有効期限をチャネル暗号鍵の変更タイミングとする。

【０１１２】

【発明の効果】

チャットクライアント間でチャネル暗号鍵を分散管理し、クライアント間で公開鍵暗号を利用して鍵の配布を行い、チャネル暗号鍵を共有する。

サーバに無関係に、クライアント間でチャネル暗号鍵を生成し、配布するので、サーバにメッセージ内容が漏洩することなく、チャネル内の会話のセキュリティを高めることが出来る。また、クライアント間で、メッセージの暗号化／復号化が行われるため、クライアント側に負荷が分散され、サーバの負荷を軽減することが出来る。

【図面の簡単な説明】

【図１】第１実施形態例に係るセキュリティ強化装置の機能ブロック図。

【図２】ユーザ情報の一例を示す説明図。

【図３】第１実施形態例に係るセキュリティ強化装置が行う主な処理の流れを示すフローチャート。

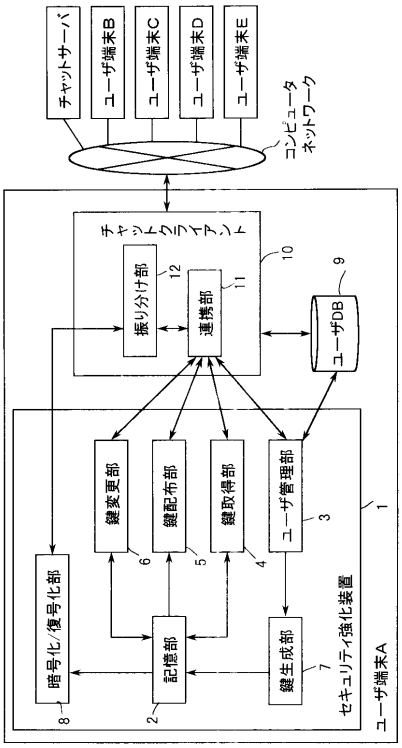
【図４】鍵取得処理の流れを示すフローチャート。

【図５】鍵配布処理の流れを示すフローチャート。

【図６】要求検証処理の流れを示すフローチャート。

【図７】鍵変更処理の流れを示すフローチャート。

【図１】

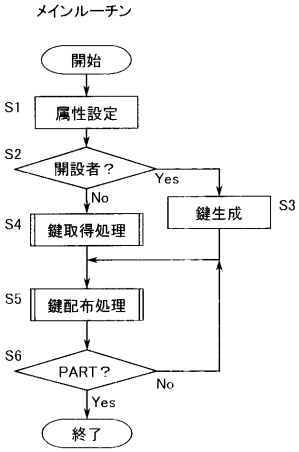


【図２】

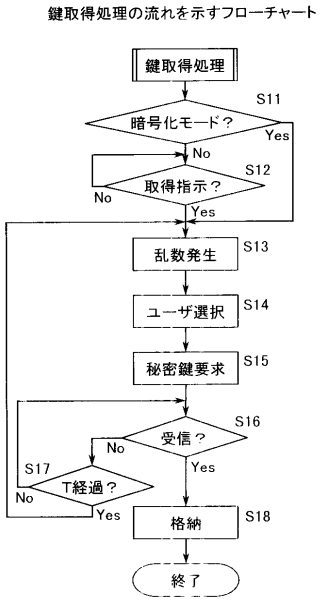
ユーザ情報の概念説明図

ニックネーム	Real Name	ユーザID	クライアント名	サーバ名	接続チャネル	アイドル時間 (sec)	Channel Operator	鍵配布 属性	鍵変更 属性	優先順位
taro	浦島 太郎	urashima	kame.ryugu.com	ryugu.com	#ryugu,#kame	90	1	1	1	1
hanako	富士通花子	fujitsu	hana.fujitsu.com	fujitsu.com	#fujitsu,#ryugu	60	1	1	1	2
…	…	…	…	…	…	…	…	…	…	…

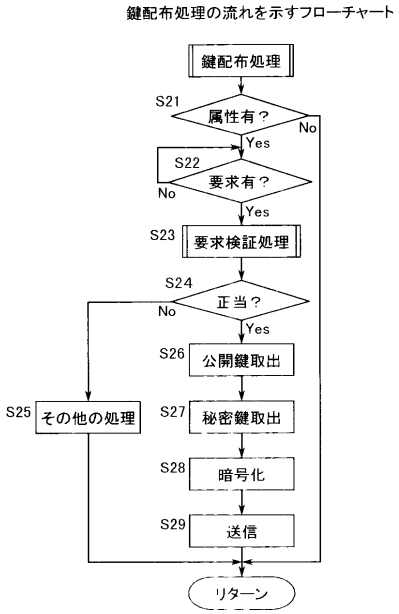
【図３】



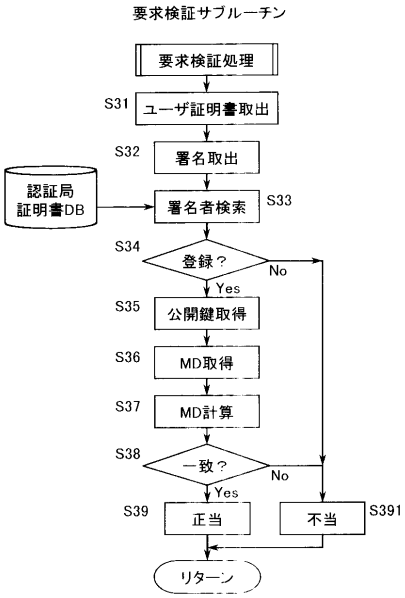
【図４】



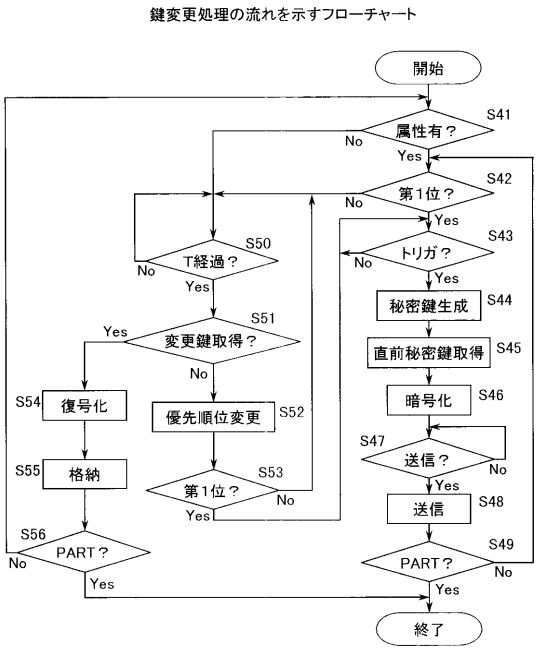
【図５】


鍵配布処理の流れを示すフローチャート
鍵配布処理
S21
属性有？
No
Yes
S22
要求有？
No
Yes
S23
要求検証処理
S24
正当？
No
Yes
S25
その他の処理
S26
公開鍵取出
S27
秘密鍵取出
S28
暗号化
S29
送信
リターン

【図６】


要求検証サブルーチン
要求検証処理
S31
ユーザ証明書取出
S32
署名取出
認証局
証明書DB
署名者検索
S33
S34
登録？
No
Yes
S35
公開鍵取得
S36
MD取得
S37
MD計算
S38
一致？
No
Yes
S39
正当
不当
S391
リターン

【図７】


鍵変更処理の流れを示すフローチャート
開始
S41
属性有？
No
Yes
S42
第1位？
No
Yes
S43
トリガ？
No
Yes
S44
秘密鍵生成
S45
直前秘密鍵取得
S46
暗号化
S47
送信？
No
Yes
S48
送信
S49
PART？
No
Yes
S50
T経過？
No
Yes
S51
変更鍵取得？
Yes
No
S52
優先順位変更
S53
第1位？
No
Yes
S54
復号化
S55
格納
S56
PART？
No
Yes
終了

フロントページの続き

(72)発明者　松井　一樹
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　石田　信行

(56)参考文献　特開平１０－０５１４３８（ＪＰ，Ａ）
特開平１０－２８９１８５（ＪＰ，Ａ）
特開平０９－０５４７４１（ＪＰ，Ａ）
特開平０６－０３７７５０（ＪＰ，Ａ）
特開平０６－２３７２４９（ＪＰ，Ａ）
特開平０６－３０３２３１（ＪＰ，Ａ）
特開平０７－０７４７４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.^{7}，ＤＢ名)
H04L　9/08
G06F 13/00