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

特許第4173924号
(P4173924)

(45)発行日　平成20年10月29日(2008.10.29)　(24)登録日　平成20年8月22日(2008.8.22)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601D
H04L 9/00 601E

請求項の数 7　(全 42 頁)

(21)出願番号　特願平10-117088
(22)出願日　平成10年4月27日(1998.4.27)
(65)公開番号　特開平11-313055
(43)公開日　平成11年11月9日(1999.11.9)
審査請求日　平成14年3月19日(2002.3.19)
審判番号　不服2005-9384(P2005-9384/J1)
審判請求日　平成17年5月19日(2005.5.19)

(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　扇　裕和
神奈川県横浜市戸塚区戸塚町２１６番地
株式会社日立製作所　宇宙技術推進本部内
(72)発明者　高島　英雄
神奈川県横浜市戸塚区戸塚町２１６番地
株式会社日立製作所　宇宙技術推進本部内
(72)発明者　高地　宗寿
神奈川県横浜市戸塚区戸塚町２１６番地
株式会社日立製作所　宇宙技術推進本部内

最終頁に続く

(54)【発明の名称】暗号通信装置、鍵管理装置および方法、ネットワーク通信システムおよび方法

(57)【特許請求の範囲】
【請求項１】
各々複数のユーザが通信に用いることができる２以上の通信ノードおよび鍵管理ノードを備えるネットワークにおいて、１の前記通信ノードを用いるユーザ（送信元ユーザと呼ぶ。）が当該通信ノードと異なる他の前記通信ノードを用いるユーザ（送信先ユーザと呼ぶ。）にデータを伝送する際に暗号化通信を行うための鍵管理方法であって、
前記鍵管理ノードは、
前記複数のユーザそれぞれを示すユーザ識別子と、当該ユーザが通信に用いることができる前記通信ノードを示す通信ノード識別子とを対応づけて管理するユーザ管理手段と、
前記通信ノードに予め与えられている復号鍵に対応づけられた暗号鍵と、当該通信ノードを示す通信ノード識別子とを対応づけて管理する通信ノード鍵管理手段と、を備え、
前記送信元ユーザから当該送信元ユーザが用いる前記通信ノードを介して送信元ユーザの識別子および送信先ユーザの識別子を含む暗号化通信の要求を受け付けると、
当該暗号化通信用のセッション鍵を生成し、
前記暗号化通信要求に含まれる送信先ユーザの識別子に対応づけて前記ユーザ管理手段に管理されている前記通信ノード識別子（送信先通信ノード識別子と呼ぶ。）を抽出し、
前記暗号化通信要求の送信元の前記通信ノードの識別子および前記送信先通信ノード識別子に対応づけて前記通信ノード鍵管理手段に管理されているそれぞれの暗号鍵を抽出し、
前記生成したセッション鍵を、それぞれの暗号鍵を用いてそれぞれ暗号化し、

暗号化後の両セッション鍵を前記暗号化通信の要求を送信した通信ノードに送信すること
を特徴とする鍵管理方法。
【請求項２】
請求項１記載の鍵管理方法であって、
前記通信ノードそれぞれは、
復号鍵と、
送信するメッセージを暗号化するスクランブル鍵および当該スクランブル鍵で暗号化したメッセージを復号するデスクランブル鍵を生成する暗号鍵生成手段と、を備え、
前記暗号化された両セッション鍵を前記鍵管理ノードから受信すると、
前記暗号鍵生成手段においてスクランブル鍵およびデスクランブル鍵を生成し、
前記受信した両セッション鍵のうち前記自身の復号鍵で復号可能な暗号鍵で暗号化された前記セッション鍵を当該自身の復号鍵で復号し、当該復号後のセッション鍵で、前記デスクランブル鍵を暗号化し、
当該暗号化後のデスクランブル鍵と、前記スクランブル鍵で暗号化したメッセージと、前記送信先ユーザが用いることができる通信ノードの復号鍵で復号可能な暗号鍵で暗号化されたセッション鍵とを、前記ネットワークに送信すること
を特徴とする鍵管理方法。
【請求項３】
各々複数のユーザが通信に用いることができる２以上の通信サーバおよび鍵管理サーバを備えるネットワークにおいて、１の前記通信サーバを用いるユーザ（送信元ユーザと呼ぶ。）が当該通信ノードと異なる他の前記通信サーバを用いるユーザ（送信先ユーザと呼ぶ。）に暗号化通信でデータを伝送する際のネットワーク通信方法であって、
前記通信サーバそれぞれは、自身を用いることができる前記ユーザそれぞれを示す識別子と、当該ユーザに予め与えられている復号鍵とを対応づけて管理する鍵管理手段と、
他の通信サーバに送信するメッセージを暗号化するスクランブル鍵および当該スクランブル鍵で暗号化したメッセージを復号するデスクランブル鍵を生成する暗号鍵生成手段と、を備え、
前記鍵管理サーバは、
前記複数のユーザそれぞれを示すユーザ識別子と、当該ユーザに予め与えられている復号鍵に対応づけられた暗号鍵とを対応づけて管理するユーザ鍵管理手段を備え、
前記送信元ユーザが用いることのできる通信サーバは、
当該送信元ユーザからメッセージとともに前記送信先ユーザへの暗号化通信の要求を受信すると、
当該受信したメッセージが暗号化されていた場合、前記鍵管理手段において当該送信元ユーザの識別子に対応づけて管理されている復号鍵で前記暗号化されたメッセージを復号し、
前記暗号鍵生成手段においてスクランブル鍵とデスクランブル鍵とを生成し、当該生成したスクランブル鍵で前記復号後のメッセージを暗号化し、
当該デスクランブル鍵を暗号化するための暗号鍵を送信先ユーザの識別子とともに前記鍵管理サーバに要求し、
デスクランブル鍵を暗号化するための暗号鍵の要求を受け取った前記鍵管理サーバは、前記ユーザ鍵管理手段に当該要求に含まれる送信先ユーザの識別子に対応づけて管理されている暗号鍵を抽出し、当該要求元の通信サーバに返信し、
前記鍵管理サーバから暗号鍵を受け取った前記通信サーバは、当該暗号鍵で前記でスクランブル鍵を暗号化し、前記暗号化したメッセージとともに送信すること
を特徴とするネットワーク通信方法。
【請求項４】
各々複数のユーザが通信に用いることができる２以上の通信サーバおよび鍵管理サーバを備えるネットワークにおいて、１の前記通信サーバを用いるユーザ（送信元ユーザと呼

ぶ。）が当該通信ノードと異なる他の前記通信サーバを用いるユーザ（送信先ユーザと呼ぶ。）に暗号化通信でデータを伝送する際のネットワーク通信方法であって、
前記通信サーバそれぞれは、自身を用いることができる前記ユーザそれぞれを示す識別子と、当該ユーザに予め与えられている復号鍵とを対応づけて管理する鍵管理手段と、
他の通信サーバに送信するメッセージを暗号化するスクランブル鍵および当該スクランブル鍵で暗号化したメッセージを復号するデスクランブル鍵を生成する暗号鍵生成手段と、を備え、
前記鍵管理サーバは、
前記通信サーバそれぞれを示す通信サーバ識別子と、当該通信サーバに予め与えられている復号鍵に対応づけられた暗号鍵とを対応づけて管理する通信サーバ鍵管理手段と、
前記通信サーバ識別子と、各通信サーバを用いることができる前記複数のユーザを示すユーザ識別子とを対応づけて管理するユーザ管理手段と、を備え、
前記送信元ユーザが用いることのできる通信サーバは、
当該送信元ユーザからメッセージとともに前記送信先ユーザへの暗号化通信の要求を受信すると、
当該メッセージが暗号化されていた場合、前記鍵管理手段において当該送信元ユーザの識別子に対応づけて管理されている復号鍵で前記暗号化されたメッセージを復号し、
前記暗号鍵生成手段においてスクランブル鍵とデスクランブル鍵とを生成し、当該生成したスクランブル鍵で前記復号後のメッセージを暗号化し、
当該デスクランブル鍵を暗号化するための暗号鍵を送信先ユーザの識別子とともに前記鍵管理サーバに要求し、
デスクランブル鍵を暗号化するための暗号鍵の要求を受け取った前記鍵管理サーバは、前記ユーザ管理手段に当該要求に含まれる送信先ユーザの識別子に対応づけて管理されている通信サーバの識別子を抽出し、前記通信サーバ鍵管理手段に抽出した前記通信サーバの識別子に対応付けられて管理されている暗号鍵を抽出し、当該要求元の通信サーバに返信し、
前記鍵管理サーバから暗号鍵を受け取った前記通信サーバは、当該暗号鍵で前記デスクランブル鍵を暗号化し、前記暗号化したメッセージとともに送信すること
を特徴とするネットワーク通信方法。

【請求項５】
各々複数のユーザが通信に用いることができる２以上の通信サーバおよび鍵管理サーバを備えるネットワークにおける通信システムであって、
前記通信サーバそれぞれは、
自身を用いることができる前記ユーザそれぞれを示す識別子と、当該ユーザに予め与えられている復号鍵とを対応づけて管理する鍵管理手段と、
自身を用いることができるユーザ（送信元ユーザと呼ぶ。）から他の通信サーバを用いることができるユーザ（送信先ユーザと呼ぶ。）へ送信するメッセージを受信すると、当該メッセージが暗号化されていた場合、前記鍵管理手段に送信元ユーザの識別子に対応づけられた管理されている復号鍵で当該メッセージを復号するネットワーク内メッセージ復号手段と、
前記ネットワークにおける暗号化通信に用いるスクランブル鍵と当該スクランブル鍵で暗号化したメッセージを復号するデスクランブル鍵を生成する暗号鍵生成手段と、
前記復号後のメッセージを前記スクランブル鍵で暗号化するメッセージ暗号化手段と、
前記メッセージの送信先ユーザを示す識別子を前記鍵管理サーバに送信するユーザ識別子送信手段と、
前記鍵管理サーバから前記ユーザ識別子送信手段から送信したユーザ識別子に対する応答として暗号鍵を受け取る暗号鍵受取手段と、
前記メッセージ暗号化手段で用いたスクランブル鍵とともに前記暗号鍵生成手段で生成したデスクランブル鍵を、前記暗号鍵受取手段で受け取った暗号鍵で暗号化する暗号鍵暗号化手段と、

前記暗号化されたメッセージと前記暗号化されたデスクランブル鍵とを前記ネットワークに送信するネットワーク送信手段と、
前記ネットワークから暗号化されたメッセージとデスクランブル鍵とを受信すると、自身に予め与えられている復号鍵で当該デスクランブル鍵を復号し、当該復号したデスクランブル鍵で前記暗号化されたメッセージを復号するメッセージ復号手段と、を備え、
前記鍵管理サーバは、
前記複数のユーザそれぞれを示すユーザ識別子と、当該ユーザが用いることができる前記通信サーバを示す通信サーバ識別子とを対応づけて管理するユーザ管理手段と、
前記通信サーバ識別子と、当該通信サーバ識別子で示される通信サーバに予め与えられている復号鍵に対応づけられた暗号鍵とを対応づけて管理する通信サーバ鍵管理手段と、
前記通信サーバから、送信先ユーザの識別子を受信すると、前記ユーザ管理手段に当該送信先ユーザの識別子に対応づけて管理されている前記通信サーバ識別子を抽出し、前記通信サーバ鍵管理手段に当該抽出した通信サーバ識別子に対応づけて管理されている前記暗号鍵を抽出し、当該暗号鍵を前記送信先ユーザの識別子の送信元の通信サーバに返信する暗号鍵抽出手段と、を備えること
を特徴とするネットワーク通信システム。

【請求項６】

各々複数のユーザが通信に用いることができる２以上の通信サーバおよび鍵管理サーバを備えるネットワークにおける通信システムであって、
前記通信サーバそれぞれは、
自身を用いることができる前記ユーザそれぞれを示す識別子と、当該ユーザに予め与えられている復号鍵とを対応づけて管理する鍵管理手段と、
自身を用いることができるユーザ（送信元ユーザと呼ぶ。）から他の通信サーバを用いることができるユーザ（送信先ユーザと呼ぶ。）へ送信するメッセージを受信すると、当該メッセージが暗号化されていた場合、前記鍵管理手段に送信元ユーザの識別子に対応づけられた管理されている復号鍵で当該メッセージを復号するネットワーク内メッセージ復号手段と、
前記ネットワークにおける暗号化通信に用いるスクランブル鍵と当該スクランブル鍵で暗号化したメッセージを復号するデスクランブル鍵とを生成する暗号鍵生成手段と、
前記復号後のメッセージを前記スクランブル鍵で暗号化するメッセージ暗号化手段と、
前記メッセージの送信先ユーザを示す送信先ユーザ識別子を前記鍵管理サーバに送信するユーザ識別子送信手段と、
前記鍵管理サーバから前記ユーザ識別子送信手段から送信したユーザ識別子に対する応答として暗号鍵を受け取る暗号鍵受取手段と、
前記メッセージ暗号化手段で用いたスクランブル鍵とともに前記暗号鍵生成手段で生成したデスクランブル鍵を、前記暗号鍵受取手段で受け取った暗号鍵で暗号化する暗号鍵暗号化手段と、
前記暗号化されたメッセージと前記暗号化されたデスクランブル鍵とを前記ネットワークに送信するネットワーク送信手段と、
前記ネットワークから暗号化されたメッセージとデスクランブル鍵とを受信すると、前記鍵管理手段に当該メッセージの送信先ユーザの識別子に対応づけて管理されている復号鍵で当該デスクランブル鍵を復号し、当該復号したデスクランブル鍵で前記暗号化されたメッセージを復号するメッセージ復号手段と、を備え、
前記鍵管理サーバは、
前記複数のユーザそれぞれを示すユーザ識別子と、当該ユーザに予め与えられている復号鍵に対応づけられた暗号鍵とを対応づけて管理するユーザ鍵管理手段と、
前記通信サーバから、前記送信先ユーザ識別子を受信すると、前記ユーザ鍵管理手段に当該送信先ユーザ識別子に対応づけて管理されている前記暗号鍵を抽出し、当該暗号鍵を前記送信先ユーザの識別子の送信元の通信サーバに返信する暗号鍵抽出手段と、を備え、
前記ユーザ識別子送信手段は、さらに、前記メッセージの送信元ユーザを示す送信元ユ

ーザ識別子も前記送信先ユーザ識別子とともに前記鍵管理サーバに送信し、
前記暗号鍵抽出手段は、セッション鍵を生成し、前記ユーザ鍵管理手段に当該送信元ユーザ識別子に対応づけて管理されている前記暗号鍵をさらに抽出し、前記抽出した送信元ユーザ識別子に対応づけて管理されている暗号鍵および送信先ユーザ識別子に対応づけて管理されている暗号鍵それぞれで、前記生成したセッション鍵を暗号化し、暗号化後の両セッション鍵（それぞれ、送信元暗号化セッション鍵、送信先暗号化セッション鍵と呼ぶ。）を前記送信元の通信サーバに返信し、
前記暗号鍵受取手段は、前記暗号鍵の代わりに、前記送信元暗号化セッション鍵および送信先暗号化セッション鍵とを受け取り、
前記暗号鍵暗号化手段は、前記暗号鍵の代わりに、前記送信元暗号化セッション鍵で前記デスクランブル鍵を暗号化し、
前記ネットワーク送信手段は、前記暗号化されたメッセージと前記暗号化されたデスクランブル鍵とに加え、前記送信先暗号化セッション鍵も送信し、
前記メッセージ復号手段は、前記前記ネットワークから暗号化されたメッセージとデスクランブル鍵と前記送信先暗号化セッション鍵とを受信すると、前記鍵管理手段に送信先ユーザ識別子に対応づけて管理されている復号鍵で、前記送信先暗号化セッション鍵を復号し、当該復号したセッション鍵で前記デスクランブル鍵を復号し、当該復号したデスクランブル鍵で前記暗号化されたメッセージを復号すること
を特徴とするネットワーク通信システム。
【請求項７】
請求項５記載のネットワーク通信システムであって、
前記ユーザ識別子送信手段は、さらに、自身の通信サーバの識別子（送信元通信サーバ識別子と呼ぶ。）を前記送信先ユーザ識別子とともに前記鍵管理サーバに送信し、
前記暗号鍵抽出手段は、セッション鍵を生成し、前記サーバ鍵管理手段に前記送信元サーバ識別子に対応づけて管理されている暗号鍵をさらに抽出し、前記送信元サーバ識別子に対応付けられて管理されている暗号鍵および送信先ユーザ識別子に対応づけて管理されている通信サーバの識別子に対応づけて管理されている暗号鍵のそれぞれで、前記生成したセッション鍵を暗号化し、暗号化後の両セッション鍵（それぞれ、送信元暗号化セッション鍵、送信先暗号化セッション鍵と呼ぶ。）を前記送信元の通信サーバに返信し、
前記暗号鍵受取手段は、前記暗号鍵の代わりに、前記送信元暗号化セッション鍵および送信先暗号化セッション鍵とを受け取り、
前記暗号鍵暗号化手段は、前記暗号鍵の代わりに、前記送信元暗号化セッション鍵で前記デスクランブル鍵を暗号化し、
前記ネットワーク送信手段は、前記暗号化されたメッセージと前記暗号化されたデスクランブル鍵とに加え、前記送信先暗号化セッション鍵も送信し、
前記メッセージ復号手段は、前記前記ネットワークから暗号化されたメッセージとデスクランブル鍵と前記送信先暗号化セッション鍵とを受信すると、自身の復号鍵で、前記送信先暗号化セッション鍵を復号し、当該復号したセッション鍵で前記デスクランブル鍵を復号し、当該復号したデスクランブル鍵で前記暗号化されたメッセージを復号すること
を特徴とするネットワーク通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
データを、情報障害を避けた状態で伝達することに好適な、暗号通信装置、鍵管理装置および方法、ネットワーク通信システムおよび方法に係り、特に、ユーザが属するグループごとに鍵を管理することに好適な、暗号通信装置、鍵管理装置および方法、ネットワーク通信システムおよび方法に関する。
【０００２】
【従来の技術】
文書データ等の情報の伝達は、紙に印刷された書類の郵便，または公衆電話網を利用した

ＦＡＸによる伝達が利用されている。
【０００３】
近年、パソコンの普及によりパソコンを公衆電話網に接続し、文書データそのものを電子メール，インターネット等により送受できるようになった。
【０００４】
情報伝達の安全性（セキュリティ）を確保する方法としては、文書作成を行うパソコンに暗号ソフトをインストールし、送受するユーザ間で伝達する文書を暗号化し通信する方法がとられる。
【０００５】
ユーザＡとユーザＢとが暗号化通信を行う場合、データを暗号化するための鍵と復号化するための鍵を定め、ユーザＡは暗号化用の鍵でデータを暗号化し、これを受信したユーザＢは復号化用の鍵で情報を復号化する。セキュリティを向上させるため、各ユーザがデータの暗号化、復号化に用いる鍵とは別の鍵をマスター鍵として所有し、情報伝達を実施するたびに、上記データの暗号化用の鍵と復号化用の鍵とをセッション鍵として生成し、ユーザＡはユーザＢにセッション鍵で暗号化したデータと、ユーザＢが復号できるようユーザＢのマスター鍵で暗号化したセッション鍵を送付する。
【０００６】
複数のユーザ間でネットワークを構築し、双方向の暗号化通信を行う場合は、専用の鍵管理局を設置して暗号に用いるマスター鍵，セッション鍵を管理すると共に、ユーザが所有するマスター鍵を利用してユーザの確認を行い、確認できないユーザのネットワーク利用を排除するアクセス管理が行われる。
【０００７】
【発明が解決しようとする課題】
ところが、上述した従来の技術では、暗号化通信が各ユーザ相互に、すなわち、マスター鍵，セッション鍵が各ユーザごとに運用される。このため、グループ間にまたがって暗号化通信が実施され、複数のユーザから構成されるグループを暗号化通信に関する１つのまとまった系とすることができない。
【０００８】
本発明は、複数のユーザから構成されるグループを暗号化通信に関する１つのまとまった系とした状態で、通信のセキュリティを確保することに好適な、暗号通信装置、鍵管理装置および方法、ネットワーク通信システムおよび方法を提供することにある。
【０００９】
【課題を解決するための手段】
上記目的を達成するために、本発明の第１の態様によれば、
各々複数のユーザが通信に用いることができる２以上のノードについて、各ノードに暗号文を復号化するための復号鍵を予め与え、ユーザ相互にデータを伝送するに際し、宛先のユーザが用いるノードに与えられた復号鍵に対応する暗号鍵を用いて暗号化通信を行うための鍵管理方法であって、
上記暗号化に用いられる暗号鍵は、上記宛先のユーザを示すユーザ識別子に基づいて、上記各ノードについて予め作成された、ノードを示すノード識別子および当該ノードに与えられた復号鍵との対応関係、ならびに、ノードを示すノード識別子および当該ノードを用いることができるユーザを示すユーザ識別子の対応関係が記述されたデータベースから検索された復号鍵と、暗号鍵および復号鍵の対応関係とから決められること
を特徴とする鍵管理方法が提供される。
【００１０】
本発明の第２の態様によれば、
各々複数のユーザが通信に用いることができる２以上のノードについて、各ノードごとに暗号文を復号化するための復号鍵を予め与え、ユーザ相互にデータを伝送するに際し、宛先のユーザが用いるノードに与えられた復号鍵に対応する暗号鍵を用いて暗号化通信を行うための鍵管理方法であって、

上記各ノードについて、ノードを示すノード識別子および当該ノードに与えられた復号鍵との対応関係、ならびに、ノードを示すノード識別子および当該ノードを用いることができるユーザを示すユーザ識別子の対応関係が記述されたデータベースを予め作成し、
発信元のユーザから、宛先のユーザを示すユーザ識別子を含む暗号化通信の要求を受け付け、
上記ユーザ識別子を用いて上記データベースから復号鍵を検索し、
上記検索した復号鍵と、暗号鍵および復号鍵の対応関係とから暗号鍵を決定し、
上記決定した暗号鍵を発信元のユーザが用いることができるノードに送付すること
を特徴とする鍵管理方法が提供される。

【００１１】

本発明の第３の態様によれば、
各々複数のユーザが通信に用いることができる２以上のノードについて、各ノードごとに暗号文を復号化するための復号鍵を予め与え、
データを発信するに際し、宛先のユーザが用いるノードにおいて、送信すべきデータを第１の暗号鍵で第１の暗号アルゴリズムを用いて暗号化して暗号化データを生成し、上記第１の暗号鍵を、上記宛先のユーザが用いることができるノードに与えられた復号鍵に対応する第２の暗号鍵で第２の暗号アルゴリズムを用いて暗号化して暗号化暗号鍵を生成し、
上記暗号化データおよび暗号化暗号鍵を送出し、
データを受信するに際し、宛先のユーザが用いるノードにおいて、受け付けたデータから暗号化暗号鍵および暗号化データを分離抽出し、当該ノードに与えられた復号鍵を用い上記第２の暗号アルゴリズムに基づいて上記暗号化暗号鍵を復号化して暗号鍵を取得し、該取得した暗号鍵を用い上記第１の暗号アルゴリズムに基づいて暗号化データを復号化してデータを取得し、該取得したデータを受信ユーザに伝達し、
上記暗号鍵を暗号化するための暗号鍵は、データを発信するに際し、データを発信しようとするユーザから宛先のユーザを示す識別子を取得し、予め作成された、ユーザおよび復号鍵の対応を示すデータベースから検索された復号鍵と、暗号鍵および復号鍵の対応関係とから決定し、
上記データベースには、各ノードについて、ノードを示す識別子および当該ノードに与えられた復号鍵の対応関係、ならびに、ノードを示す識別子および当該ノードを用いることができるユーザの対応関係が予め登録されていること
を特徴とする鍵管理方法が提供される。

【００１２】

本発明の第４の態様によれば、
暗号化／復号化機能を有し、各々複数のユーザが登録される通信サーバが２台以上接続されて構成されるネットワークで暗号化通信を行うためのネットワーク通信方法であって、
第１のユーザから第２のユーザにデータを伝送するに際し、
上記第１のユーザが登録されている第１の通信サーバに、上記第２のユーザが登録されている第２の通信サーバに予め与えられた復号鍵に対応する暗号鍵を与え、上記第１のユーザから第２のユーザに伝送されるべきデータを、上記第１の通信サーバにおいて上記与えた暗号鍵で暗号化した状態で送出し、
上記第２の通信サーバに到来したデータを当該第２の通信サーバに予め与えられた復号鍵で復号化すること
を特徴とするネットワーク通信方法が提供される。

【００１３】

本発明の第５の態様によれば、
各々複数のユーザが登録された２以上の通信サーバが接続されて構成されるネットワーク通信システムであって、
上記各通信サーバは、
暗号鍵を管理するための鍵管理サーバと接続され、予め与えられた復号鍵で暗号文を復号化するための復号化機能と、上記鍵管理サーバから与えられた暗号鍵で暗号文を暗号化す

るための暗号化機能とを備え、
当該通信サーバに登録されているユーザからネットワーク上にデータを送出するに際し、
データの宛先となるユーザの識別子を上記鍵管理サーバに与え、
上記鍵管理サーバは、上記与えられた識別子が示すユーザが登録されている通信サーバに予め与えられた復号鍵に対応する暗号鍵を、上記識別子を与えた通信サーバに与え、
上記暗号鍵を与えられた通信サーバは、送出すべきデータを上記与えられた暗号鍵で暗号化してネットワーク上に送出すること
を特徴とするネットワーク通信システムが提供される。

【００１４】

本発明の第６の態様によれば、
各々複数のユーザが登録された通信サーバが２以上接続されて構成されるネットワークにおける暗号化通信の暗号鍵を管理するための鍵管理装置であって、
ネットワーク上に接続される各通信サーバの識別子と、該各通信サーバに予め与えられた復号鍵との対応関係、および、各通信サーバの識別子と該各通信サーバに登録された複数のユーザとの対応関係が登録されたデータベースを備え、
通信サーバから送信先ユーザを示すユーザ識別子が与えられたとき、当該ユーザ識別子が示すユーザが登録された通信サーバに与えられた復号鍵に対応する暗号鍵を、当該ユーザ識別子を与えた通信サーバに与えること
を特徴とする鍵管理装置が提供される。

【００１５】

本発明の第７の態様によれば、
各々複数のユーザが登録された通信サーバが２以上接続されて構成されるネットワークにおける暗号化通信の暗号鍵を管理するための鍵管理装置であって、
ネットワークへのアクセス権を有する複数のユーザの識別子に、各ユーザがネットワークにアクセスする拠点となる通信サーバに予め与えられた復号鍵が対応づけて登録されたデータベースを備え、
通信サーバから宛先のユーザを示すユーザ識別子が与えられたとき、当該ユーザ識別子に対応づけられた復号鍵に応じた暗号鍵を当該通信サーバに与えることを特徴とする暗号鍵管理装置が提供される。

【００１６】

本発明の第８の態様によれば、
ネットワークを介して暗号化通信を行うための暗号化通信装置であって、
双方向の通信を行うための通信手段と、
伝送すべき第１のデータを暗号化／復号化するための暗号化手段および復号化手段と、
上記第１のデータの伝送に先だって、第１のデータを暗号化するための暗号鍵を外部から取得するための暗号鍵取得手段とを備え、
上記暗号鍵取得手段は、第１のデータが伝送されるべき宛先のユーザを示す識別子を鍵管理のための情報処理装置に送出して、かつ、鍵管理のための情報処理装置から与えられる暗号鍵を受け付け、当該受け付けた暗号鍵を上記暗号化手段に与える機能を有すること
を特徴とする暗号化通信装置が提供される。

【００１７】

【発明の実施の形態】
以下、図面を参照して、本発明の実施の形態について説明する。

【００１８】

まず、図１を参照して、本発明を適用したネットワーク通信システムについて説明する。

【００１９】

図１において、複数のユーザで構成されるグループがＮ箇所存在するものとし、このグループ単位ごとに双方向の通信管理機能を持つネットワーク通信管理用ワークステーション（通信サーバ）１１０＜１＞～＜Ｎ＞を設置する。各ネットワーク通信管理用ワークステーション１１０＜１＞～＜Ｎ＞には、各グループに属するユーザがネットワークにアクセ

スするための情報処理装置１２０＜１－１＞～＜１－Ｍ１＞～＜Ｎ－ＭＮ＞（ただし、Ｍ１からＭＮは、各グループ（１～Ｎ）に属するユーザの数を示す。）が接続されている。情報処理装置１２０＜１－１＞～＜１－Ｍ１＞～＜Ｎ－ＭＮ＞は、各グループに属する複数のユーザによって情報処理装置端末として使用され、様々な情報処理装置が利用される。情報処理装置１２０＜１－１＞～＜１－Ｍ１＞～＜Ｎ－ＭＮ＞を上記ネットワーク通信管理用ワークステーション１１０＜１＞～＜Ｎ＞に接続し、ネットワーク通信システムが構築される。各ユーザは、上記通信ネットワークを利用して、文書データや、映像データを中心とする情報を双方向に伝達することができる。

【００２０】

このネットワーク通信管理用ワークステーション１１０＜１＞～＜Ｎ＞に衛星通信局設備１１２＜１＞～＜Ｎ＞を接続し、衛星通信回線８１を介して各グループを結ぶと共にに、上記ワークステーションをインターネット８２に接続し、地上通信回線８３と衛星通信回線８１をあわせて、通信ネットワークを構築する。

【００２１】

ネットワーク通信管理用ワークステーション１１０＜１＞～＜Ｎ＞は、ユーザの要求に応じて伝達するデータの暗号化および復号化する機能とともに、１対１の個別配信や、同時にＭ箇所に配信する１：Ｍの同報通信機能を有し、暗号化による双方向通信を管理している。

【００２２】

このネットワーク通信システムには、鍵管理局４０が設置されている。

【００２３】

鍵管理局４０は他の情報拠点と同様に、衛星通信局設備１１２ａとネットワーク通信管理用ワークステーション１１０ａを所有しており、これに鍵管理を実施する鍵管理用ワークステーション１４０が接続し、暗号化通信に関与する鍵の管理を行っている。

【００２４】

ここで、図２を参照して、ネットワーク通信システムを利用するユーザの情報処理装置の接続例について説明する。各グループのユーザは様々な情報を生産し、使用する情報処理装置も多岐に渡っている。

【００２５】

図２において、使用される情報処理装置１２０としては、複数のユーザが使用しているパーソナルコンピュータ１２１，様々の設計・製造データの作成に使用するＣＡＤ用ワークステーション１２２，打ち合わせ等に使用するＴＶ会議用パーソナルコンピュータ１２３，メールサーバ１２４等がある。

【００２６】

これらの情報処理装置とネットワーク通信管理用ワークステーションとは、ＬＡＮ（local area network；ローカルエリアネットワーク）１３０で接続している。

【００２７】

鍵管理局４０は、独立してネットワーク通信管理用ワークステーション１１０ａを使用することもできるが、通信回線に余裕がある場合は、他のグループのユーザがルータ１８１を経由して、鍵管理局４０のネットワーク通信管理用ワークステーション１１０ａに接続することも可能である。

【００２８】

次に、図３を参照して、本発明を適用したネットワーク通信システムにおける、通信に関するデータの制御および処理について説明する。

【００２９】

この制御および処理は、各グループに設置されたネットワーク通信管理用ワークステーション、鍵管理局の鍵管理用ワークステーション、および各ユーザが使用するパーソナルコンピュータなどの情報処理装置により実施される。本発明を適用したネットワーク通信システムの通信に関する制御および処理は、大きく分けて、アクセス管理部１０１０と、ネットワーク通信管理部１０２０と、暗号化通信処理部１０３０と、鍵管理部１０４０と、

否認防止管理部１０５０と、鍵回復部１０６０とを有して構成される。

【００３０】

上記アクセス管理部１０１０は、ユーザがパーソナルコンピュータ等の情報処理装置からネットワーク通信システムを利用しようとした場合、ユーザ認証として、システムからこのユーザに割り当てられているマスター鍵を所有しているかどうかの確認を実施し、ユーザの不正なアクセスを排除するアクセス管理を実施するためのものである。

【００３１】

上記ネットワーク通信管理部１０２０は、データを発信するユーザの要求に応じて、送受信設備を発信先の相手ユーザと接続し、ユーザの必要に応じて、１対１の個別配信または、同時にM箇所に配信する１：Ｎの同報通信を行うための送受信管理を実施するためのものである。

【００３２】

上記暗号化通信処理部１０３０は、発信するユーザ側で、伝達するデータを暗号化して送信し、受信側でこれを復号化してデータを取得する暗号化通信処理を実施するためのものである。

【００３３】

上記鍵管理部１０４０は、暗号化通信に関与する鍵の生成、更新、削除、およびネットワーク利用者に対する鍵の配布に関する鍵管理を実施するためのものである。

【００３４】

上記否認防止管理部１０５０は、ユーザが伝達するデータに対して、変造、偽造、不到達等の情報損失や、通信の当事者が実施した通信行為に対する否認を防止するための管理を実施するためのものである。

【００３５】

上記鍵回復部１０６０は、鍵の紛失、不正使用等、不測の事態が発生し通信された暗号文を解読する必要が生じた場合、鍵を回復し暗号文の復号を実施するためのものである。

【００３６】

次に、同じく図３を参照して、本発明のネットワーク通信システムにおける各制御処理部の処理の概要について説明する。ここでは、ユーザＡからユーザＢへ暗号化通信を行う場合をを例に挙げて説明する。

【００３７】

（１）　ユーザＡは、本発明のネットワーク通信システムにアクセスするため、使用するユーザが使用するパーソナルコンピュータの電源を投入する。すると、アクセス管理部１０１０が動作し、ユーザＡが正当なユーザか否かを判断（確認）するためのユーザ認証を実施する。

【００３８】

正当なユーザと判断された場合、ユーザＡは初めて、ネットワーク通信システムにアクセスすることが許可され、暗号化通信や送付されたデータを見ることができる。

【００３９】

（２）　暗号化通信を実施する場合、ユーザＡはアクセス管理部１０１０に送信するデータと送信先相手の宛先を入力する。入力データと宛先とは、ネットワーク通信管理部１０２０に送られ、送信先相手と通信装置とを接続し、通信経路を確立する。

【００４０】

（３）　データは、暗号化通信処理部１０３０に送られ、鍵管理部１０４０が発行した鍵を用いて暗号化され暗号文が作成される。作成された暗号文は、確立された通信経路に沿って送信先相手に伝達される。暗号文を受信した送信先相手は、鍵管理部１０４０が発行した鍵をもとにデータを復号し、取得したデータをネットワーク通信管理部１０２０に送付する。

【００４１】

（４）　ユーザＢに対してもアクセス管理部１０１０によりユーザ認証が実施され、ユーザＢが正当なユーザと確認された場合、得られたデータはネットワーク通信管理部１０２

０からアクセス管理部１０１０を経由してユーザＢに伝達される。
【００４２】
（５）　鍵管理部１０４０は、暗号化通信処理部１０３０が使用する鍵のみならず、アクセス管理部１０１０がユーザ認証に使用する鍵についての管理、すなわち、鍵の登録、更新および削除を行う。
【００４３】
（６）　ユーザＡからユーザＢに伝達されるデータに対して、否認防止に関する判定結果を必要とする場合、アクセス管理部１０１０に送信するデータを入力する際、同時に否認防止判定要求の入力を行う。
【００４４】
すると、否認防止管理部１０５０が動作し、暗号化通信の前後で変造、偽造、不到達等の異常が発生したかどうかの判定を行う。
【００４５】
ユーザＡ，Ｂは、データ通信が終了してから否認防止管理部１０５０にアクセスすると、否認防止に関する判定結果を取得することができる。
【００４６】
（７）　不測の事態（例えば、鍵の紛失、不正使用等）が発生し、通常の暗号化通信経路によらず暗号文を復号する必要が生じた場合、鍵回復部１０６０に暗号文と鍵回復要求とを入力すると、暗号文を復号することができる。
【００４７】
本発明のネットワーク通信システムを構成するこの６つの制御処理は、ネットワーク通信システム上の各情報処理装置（例えば、図２に示される、各グループに設置されたネットワーク通信管理用ワークステーションとそれに接続するパーソナルコンピュータなどのユーザが使用する情報処理装置、および鍵管理局の鍵管理用ワークステーション）におけるソフト処理により実現される。
【００４８】
次に、図４を参照して、ユーザが使用するパーソナルコンピュータなどの情報処理装置、ネットワーク通信管理用ワークステーション、鍵管理用ワークステーションに組み込まれるソフト機能について説明する。
【００４９】
（１）　ユーザが使用するパーソナルコンピュータなどの情報処理装置１２０は、ユーザセキュリテイ機能ｆ２１と、データファイル処理機能ｆ２２とを備える。
【００５０】
上記ユーザセキュリテイ機能ｆ２１は、ユーザのアクセス管理するためのユーザ認証の環境と、相手ユーザと接続するための操作環境とを提供するためのものである。
【００５１】
上記データファイル処理機能ｆ２２は、ユーザが個別または、同時に複数のユーザに対して、問い合わせ、伝達を行うための環境と、問い合わせ内容、伝達内容の設定、送信、回答結果の受信、回答結果の表示、および、任意のユーザにファイルを転送する操作環境とを提供するためのものである。
【００５２】
（２）　ネットワーク管理用ワークステーション１１０は、通信セキュリテイ管理機能ｆ１と、ネットワーク送受信管理機能ｆ１２と、スクランブル機能ｆ１３と、デスクランブル機能ｆ１４と、通信構成管理機能ｆ１５とを備える。
【００５３】
上記通信セキュリテイ管理機能ｆ１１は、ユーザからのユーザ認証要求に対する認証判定を暗号アルゴリズムにより実施し、また、相手ユーザと暗号化通信を実施する場合、暗号化通信要求が発生するごとに鍵管理ワークステーション１４０よりセッション鍵の受信し、暗号化通信を実施するためのものである。
【００５４】

上記ネットワーク送受信管理機能ｆ１２は、ネットワーク管理用ワークステーション１１０相互に通信を実施するために、相手ユーザと接続し、通信経路の確立を行うためのものである。

【００５５】

上記スクランブル機能ｆ１３は、ネットワーク管理用ワークステーション１１０間で行われる通信において、送信データの暗号化と暗号化に必要な鍵の生成、およびこの鍵を配信するためのものである。

【００５６】

上記デスクランブル機能ｆ１４は、ネットワーク管理用ワークステーション１１０間で行われる通信において、受信データの復号化と、復号化に必要な鍵の受信およびこれを生成するためのものである。

【００５７】

上記通信構成管理機能ｆ１５は、ネットワーク管理用ワークステーション１１０で使用するデータベースの検索、登録、削除を行うためのものである。ネットワーク管理用ワークステーション１１０では、例えば、アクセスするユーザを管理するためのユーザＩＤデータベース１１、ユーザ鍵管理データベース１２を使用する。これらのデータベースの内容については後述する。

【００５８】

（３）　鍵管理用ワークステーション４０は、鍵構成管理機能ｆ４１と、否認防止機能ｆ４２と、鍵回復機能ｆ４３とを備える。鍵管理用ワークステーション４０では、例えば、ネットワークを使用するユーザを管理するためのネットワークユーザＩＤデータベース２５、ネットワーク上の暗号化通信に用いる暗号鍵を管理するためのネットワーク鍵構成データベース２４、および、否認を防止するための情報を格納した否認防止データベース（図示せず）を使用する。これらのデータベースの内容については後述する。

【００５９】

上記鍵構成管理機能ｆ４１は、暗号化通信に関与する鍵の発行、生成、更新、削除に関する鍵管理を実施するためのものである。

【００６０】

上記否認防止機能ｆ４２は、ユーザが実施するデータの送受信に対し、変造、偽造がなかったか、第３者としての公平な立場で、否認防止の判定を行うためのものである。

【００６１】

上記鍵回復機能ｆ４３は、鍵の紛失、不正使用という不測の事態が発生した場合、鍵を回復し通信に用いられる暗号文を復号するためのものである。

【００６２】

以下に、上記本発明のネットワーク通信システムの６つの制御処理部を、上記に示すコンピュータ、および、それに組み込まれたソフト機能で実現した実施例について説明する。

【００６３】

この実施例では、データの暗号化、復号化に用いるスクランブル鍵、デスクランブル鍵を運用する暗号アルゴリズムは、共通鍵暗号アルゴリズムを使用している。

【００６４】

ユーザに所有させるマスター鍵の生成、および、生成された鍵を配送するに際し使用する暗号アルゴリズムは、共通鍵暗号アルゴリズム、公開鍵暗号アルゴリズムのどちらでもシステムを構築することが可能である。

【００６５】

まず、共通鍵暗号アルゴリズムを用いた実施例を示し、その後で、公開鍵暗号アルゴリズムを用いた実施例について説明する。

【００６６】

まず、図３、４および図５を参照して、共通鍵暗号アルゴリズムを用いた、アクセス管理部のソフト機能構成の実施例について説明する。

【００６７】

共通鍵暗号アルゴリズムとしては、例えば、ＭＵＬＴＩ４暗号アルゴリズムなどを用いることができる。ＭＵＬＴＩ４暗号アルゴリズムは、アルゴリズム決定鍵およびデータ鍵に基づき暗号化／復号化関数の決定を行う処理と、データの暗号化／復号化を行う処理との２段階に分けられた暗号処理を行う。この処理の内容については、例えば、特開平０４－１７０５７６号公報などに記載されている。

【００６８】

図４において、アクセス管理部１０１０（図３参照）を運用するため、パーソナルコンピュータなどの情報処理装置１２０を使用する各ユーザには、あらかじめ鍵管理局４０より、ユーザＩＤとマスター鍵としての秘密鍵が割り当てられている。

【００６９】

このユーザＩＤは、ネットワーク通信管理用ワークステーション１１０のユーザＩＤデータベース１１に登録し、マスター鍵としての秘密鍵は、ネットワーク通信管理用ワークステーション１１０のユーザ鍵管理データベース１２に、ユーザＩＤと対応させてユーザのマスター鍵として登録している。

【００７０】

アクセス管理部１０１０（図３参照）では、ユーザが使用するパーソナルコンピュータなどの情報処理装置１２０のユーザセキュリテイ機能ｆ２１とネットワーク通信管理用ワークステーション１１０の通信セキュリテイ機能ｆ１１との暗号化通信によって、ユーザ認証を実施する。

【００７１】

以下、図５を参照して、この実施例について説明する。

【００７２】

（１）　ユーザが、本ネットワーク通信システムを利用する場合、ユーザが使用するパーソナルコンピュータなどの情報処理装置１２０にアクセス要求５０１を入力する。ユーザセキュリテイ機能ｆ２１は、「シーケンス番号」５０５を付加しユーザ認証要求５０３として通信セキュリテイ機能ｆ１１に送付する。

【００７３】

（２）　この要求を受けて、通信セキュリテイ機能ｆ１１は「ユーザＩＤ」５０６をキーとしてユーザＩＤデータベース１１を検索し、「ユーザＩＤ」５０６が該当すれば、まず、時刻情報（「月」、「日」、「時」、「分」、「秒」）と乱数から構成される、チャレンジコード$CAC_0$５０７を生成し、次に「ユーザＩＤ」５０６をキーとして、ユーザ鍵管理データベース１２を検索し当該ユーザに割り当てられた「ユーザマスタ鍵」P_{ID}５０８を取得する。

【００７４】

そして、この「ユーザマスタ鍵」P_{ID}５０８によりチャレンジコード$CAC_0$５０７を暗号化し暗号化チャレンジコードE_{PID}（CAC_0）５０９を作成し、ユーザセキュリテイ機能ｆ２１に送付する。

【００７５】

（３）　ユーザは、フロッピーデイスクまたはＩＣカードなどの記憶媒体に、当該ユーザに割り当てられたユーザマスタ鍵５０８を保管しており、この鍵を入力しすることにより、送付された暗号化チャレンジコードE_{PID}（CAC_0）５０９を復号しチャレンジコードＣＡＣ５１０を生成する。

【００７６】

そして、この生成したチャレンジコードＣＡＣ５１０を通信セキュリテイ機能に送り返す。

【００７７】

（４）　通信セキュリテイ機能ｆ１１は、ここの機能で生成されたチャレンジコード$CAC_0$５０７と復号されて送付されたチャレンジコードＣＡＣ５１０とを比較し、両者が一致すれば、ユーザを正当なユーザと判断し、認証判定結果を認証完了とする。逆に、両者が一致しなければ、認証判定結果を認証エラーとし、この認証判定結果をユーザセキュリ

テイ機能ｆ２１に送付する。
【００７８】
（５）　ユーザセキュリテイ機能ｆ２１は、認証判定結果がユーザ認証完了の場合、「シーケンス番号」５０５を除いてユーザ認証結果としネットワーク通信管理部に伝達する。
【００７９】
次に、図４を参照して、ネットワーク通信管理部１０２０（図３参照）のソフト機能構成の実施例について説明する。
【００８０】
図４に示される、ユーザは使用するパーソナルコンピュータなどの情報処理装置１２０のデータファイル処理機能ｆ２２にデータを入力し、この機能から入力されたデータはネットワーク通信管理用ワークステーション１１０のネットワーク送受信管理機能ｆ１２に送られる。このネットワーク通信管理用ワークステーション１１０でユーザの要求に応じてデータが処理され送信先相手側に送付され、ネットワーク通信管理用ワークステーション１１０のネットワーク送受信管理機能ｆ１２を経由して、送信先相手ユーザに伝達される一連の処理がネットワーク通信管理部によって管理される。
【００８１】
以下、図３、４を参照して、このネットワーク通信管理部の実施例について説明する。
【００８２】
（１）ユーザが同時に複数のユーザに対して問い合わせを行う場合、
（ｉ）ユーザが起動指示を行い、問い合わせ内容作成要求をデータファイル処理機能ｆ２２に入力する。
【００８３】
（ｉｉ）ウィンドウ画面上に入力画面が表示され、問い合わせ内容，および宛先が入力可能となる。
【００８４】
（ｉｉｉ）問い合わせ内容送信要求を入力すると、ネットワーク送受信管理機能ｆ１２に同報データとして送付し、データ識別子を付加して暗号化通信処理部１０３０に送付する。
【００８５】
（２）ユーザが同時に複数のユーザに対して、回答を行う場合、
（ｉ）ユーザが起動指示を行い、回答内容作成要求をデータファイル処理機能ｆ２２に入力する。
【００８６】
（ｉｉ）ウィンドウ画面上に入力画面が表示され、回答内容，および宛先を入力が入力可能となる。
【００８７】
（ｉｉｉ）回答送信要求を入力すると、ネットワーク送受信管理機能ｆ１２に回答データとして送付し、データ識別子を付加して、暗号化通信処理部１０３０に送付する。
【００８８】
（３）ユーザが同時に複数のユーザに対して伝達を行う場合、
（ｉ）ユーザが起動指示を行い、伝達内容作成要求をデータファイル処理機能ｆ２２に入力する。
【００８９】
（ｉｉ）ウィンドウ画面上に入力画面が表示され、伝達内容，および宛先が入力可能となる。
【００９０】
（ｉｉｉ）伝達内容送信要求を入力すると、ネットワーク送受信管理機能ｆ１２に伝達データとして送付し、データ識別子を付加して、暗号化通信処理部１０３０に送付する。
【００９１】
（４）ユーザが同時に複数のユーザに対してファイル転送を行う場合、

（ｉ）ユーザが起動指示を行い、ファイル転送要求をデータファイル処理機能ｆ２２に入力する。

【００９２】

（ｉｉ）ファイル名および宛先を入力すると、データベースからファイルが読み込まれる。

【００９３】

（ｉｉｉ）ネットワーク送受信管理機能ｆ１２にファイル転送データとして送付し、暗号化通信処理部１０３０に送付する。

【００９４】

以上のシーケンスで、問い合わせ内容の設定，送信，回答内容の設定，送信，伝達内容の設定，送信，転送ファイルの設定，送信が実施され、画面上に送信内容が表示される。問い合わせ内容の受信，回答結果の受信，伝達内容の受信，転送ファイルの受信も同様のシーケンスで実施され、画面上には、受信内容が表示される。

【００９５】

次に、図６を参照して、共通鍵暗号アルゴリズムを使用した場合の暗号化通信処理部のソフト機能構成の実施例について説明する。

【００９６】

暗号化通信を実施する場合、図４のネットワーク通信システムに組み込まれるソフト機能に示すように、ネットワーク通信管理用ワークステーション１１０のスクランブル機能は、ネットワーク送受信管理機能から送信するデータを受け取る。次に、鍵管理用ワークステーションの鍵構成管理機能からセッション鍵の発行を受け、この鍵をもとに受け取ったデータを暗号化し暗号文を作成し、送信先相手ユーザ側のネットワーク通信管理用ワークステーションのデスクランブル機能に送信する。

【００９７】

デスクランブル機能は、送付された暗号文を復号化し、データを取得する。

【００９８】

暗号化通信処理部を運用する前提条件として前述のアクセス管理部と同様、パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理局よりユーザＩＤとマスター鍵としての秘密鍵が割り当てられており、鍵管理用ワークステーションのネットワーク鍵構成データベースに、ユーザに割り当てたマスター鍵をユーザＩＤと対応させて登録し管理している。同様にネットワーク通信管理用ワークステーションのユーザ鍵管理データベースにユーザＩＤとマスター鍵とを対応させて登録しているものとする。

【００９９】

以下に、この暗号化通信処理部の実施例について説明する。

【０１００】

（１）　暗号化通信要求が発生すると、鍵管理用ワークステーション１４０の鍵構成管理機能ｆ４１は、セッション鍵P_T６０１を生成する。次に、送信側のユーザのマスター鍵P_{ID}６０２、受信側のユーザのマスター鍵P_{ID}６０３をネットワーク鍵構成データベース２４より取り出し、セッション鍵P_T６０１を平文として暗号化を行い、暗号文E_{PID}（P_T）６０４、E_{PYID}（P_T）６０５を作成する。この暗号文を発信側ユーザの使用するパーソナルコンピュータなどの情報処理装置と接続するネットワーク通信管理用ワークステーション１１０に送付する。

【０１０１】

（２）発信側のユーザの接続するネットワーク通信管理用ワークステーション１１０では、管理しているユーザのマスター鍵P_{ID}６０３をユーザ鍵管理データベース１２より取り出し、この鍵を用いて、暗号化されて送付されたセッション鍵を復号し、セッション鍵P_Tを取得する。

【０１０２】

（３）一方、発信側のユーザの接続するネットワーク通信管理用ワークステーション１１０では、ユーザが入力したデータＭをネットワーク送受信管理機能ｆ１２から受け取り、

このデータMを暗号化するためのスクランブル鍵K_S６０６、復号化するためのデスクランブル鍵K_D６０７を生成する。

【０１０３】

（４）次に、ユーザが入力したデータMをスクランブル鍵K_S６０６で暗号化し、暗号文E_{KS}（M）６０８を作成し、同様にデスクランブル鍵K_D６０７をセッション鍵P_Tで暗号化し、暗号文E_{PT}（K_S）６０９を作成する。この作成した２組の暗号文と、送付された暗号文E_{PYID}（P_T）６０５とを送信先相手のユーザの使用するパーソナルコンピュータなどの情報処理装置が接続するネットワーク通信管理用ワークステーション１１０に送信する。

【０１０４】

（５）送信先相手ユーザ側のネットワーク通信管理用ワークステーション１１０は、このユーザのマスター鍵P_{YID}６０３をユーザ鍵管理データベース１２より取り出し，この鍵を用いて送付された暗号化セッション鍵E_{PYID}（P_T）６０５を復号し、セッション鍵P_T６０１を取得する。次に、送付された暗号化デスクランブル鍵E_{PT}（K_D）６０８を上記取得したセッション鍵P_T６０１を用いて復号し、デスクランブル鍵K_D６０７を取得する。

【０１０５】

最後に、このデスクランブル鍵K_D６０７を用いて送付されたデータの暗号文E_{KS}（M）６０８を復号し、データMを取得する。

【０１０６】

（６）取得したデータは、ネットワーク送受信管理機能を経由して送信先相手ユーザに伝達される。

【０１０７】

以上の方式で、ユーザからユーザへの暗号化通信を実施する。スクランブル鍵K_S６０６、デスクランブル鍵K_D６０７を運用するアルゴリズムとして、ＣＳディジタル放送で実績のあるＭＵＬＴＩ２暗号アルゴリズムを使用し、マスター鍵６０２，６０３およびセッション鍵６０１を運用するアルゴリズムとして、ＭＵＬＴＩ２とは異なるＭＵＬＴＩ４の暗号アルゴリズムを用いるものとする。

【０１０８】

このようにして、データの暗号化に用いるスクランブル鍵K_S６０６の暗号アルゴリズムと、デスクランブル鍵K_D６０７の配送に用いるセッション鍵６０１の暗号アルゴリズムとを、異なった暗号アルゴリズムとする二重暗号化方式を取ることが可能となる。従って、同一の暗号アルゴリズムを使用する場合とくらべてセキュリティの向上を図ることができる。

【０１０９】

次に、図７を参照して、本発明を適用したネットワーク通信システムの鍵管理部のソフト機能構成の実施例について説明する。

【０１１０】

鍵管理部１０４０（図３参照）は、アクセス管理部１０１０（図３参照）、暗号化通信処理部１０３０（図３参照）の実施例で述べたように、本ネットワーク通信システムを使用する全てのユーザのマスター鍵および、暗号化通信に関与するセッション鍵を管理しており、鍵管理用ワークステーション１４０のネットワーク鍵構成データベース２４に全てのユーザのマスター鍵をユーザＩＤに対応させて登録している。

【０１１１】

また、ネットワーク通信管理用ワークステーション１１０のユーザ鍵管理データベース１２には、このネットワーク通信管理用ワークステーション１１０と接続するユーザのマスター鍵をユーザＩＤに対応させて登録している。

【０１１２】

以下、図７を参照して、この鍵管理部の実施例について説明する。

【０１１３】

（１）セッション鍵の管理
（ｉ）　暗号化通信処理部１０３０（図３参照）で暗号化通信を行う場合、発信側ユーザのネットワーク通信管理用ワークステーション１１０の通信セキュリティ管理機能ｆ１１から、発信側のユーザＩＤと送信先相手のユーザＩＤを付加したセッション鍵発行要求７０１が、鍵管理ワークステーション１４０の鍵構成管理機能ｆ４１に送付される。
【０１１４】
（ｉｉ）　鍵構成管理機能ｆ４１は、この要求を受けセッション鍵P_Tを生成するとともに、ユーザＩＤをキーとしてネットワーク鍵構成データベース２４を検索し、発信側ユーザのマスター鍵P_{ID}、送信先相手ユーザのマスター鍵P_{YID}を取り出す。次に、P_Tを平文として暗号化し、暗号化セッション鍵$E_{PID}(P_T)$、$E_{PYID}(P_T)$を作成し、発信側ユーザのネットワーク通信管理用ワークステーション１１０の通信セキュリティ管理機能ｆ１１に発行する。
【０１１５】
（ｉｉｉ）　暗号化セッション鍵を受信した通信セキュリティ管理機能ｆ１１は、発信側ユーザのユーザＩＤをキーとしてユーザ鍵管理データベース１２を検索し、ユーザのマスター鍵P_{ID}を取り出す。次に、このマスター鍵をもとに暗号化セッション鍵$E_{PID}(P_T)$を復号化し、セッション鍵P_Tを取得する。
【０１１６】
以上のシーケンスにより、発信側のユーザが接続するネットワーク通信管理用ワークステーション１１０に、セッション鍵P_Tと暗号化セッション鍵$E_{PYID}(P_T)$が発行される。
【０１１７】
（２）マスター鍵の管理
ユーザのマスター鍵は、鍵管理用ワークステーション１４０の鍵構成管理機能ｆ４１と、ネットワーク通信管理用ワークステーション１１０の通信構成管理機能ｆ１５により管理されており、ユーザのマスター鍵の登録、更新、削除はこれらの機能により実施される。
【０１１８】
ネットワーク通信管理用ワークステーション１１０設置時、このワークステーションにネットワークＩＤとネットワークマスター鍵を割り当て、通信構成管理機能ｆ１５によりユーザ鍵管理データベース１２に登録するとともに、鍵管理用ワークステーション１４０の鍵構成管理機能ｆ４１よりネットワーク鍵構成データベース２４に登録する。
【０１１９】
各ユーザのマスター鍵は、鍵構成管理機能ｆ４１が生成し、生成したマスター鍵とユーザＩＤを対応させてネットワーク鍵構成データベース２４に登録する。
【０１２０】
このユーザのマスター鍵は、ネットワーク通信管理用ワークステーション１１０のユーザ鍵管理データベース１２に登録する必要があるが、この登録は、ネットワーク通信管理用ワークステーション１１０設置時、通信構成管理機能ｆ１５より直接入力しユーザ鍵管理データベース１２に登録することもできるが、上記ネットワーク通信管理用ワークステーション１１０に割り当てたネットワークマスター鍵を使用し、スクランブル機能で暗号化して配送することもできる。同様に、ユーザのマスター鍵および、ネットワークマスター鍵の更新、削除に関するデータも上記ネットワーク通信管理用ワークステーション１１０に割り当てたネットワークマスター鍵を使用し、スクランブル機能で暗号化して、マスター鍵更新要求７０３として配送することもできる。
【０１２１】
ネットワーク通信管理用ワークステーション１１０は、送付された鍵の登録、更新、削除に関するデータを復号化し、通信構成管理機能ｆ１５によりユーザ鍵管理データベース１２の鍵の登録、更新、削除を実施する。
【０１２２】
各ユーザへのマスター鍵の更新、および配布は、ネットワーク通信管理用ワークステーション１１０側でＩＣカードまたはフロッピーディスクなどの記憶媒体に記録してオフライ

ンで配布するか、変更前のユーザに割り当てられたマスター鍵で暗号化し、ネットワークを利用してオンラインで送付することができる。これらのうち、どちらの方式をとるかは、状況によって定めればよい。

【０１２３】

次に、図８を参照して、否認防止部のソフト機能構成の実施例について説明する。

【０１２４】

ユーザが他の相手ユーザにデータを送信する場合、ネットワーク通信管理部１０２０（図３参照）の実施例で説明したように、ユーザはパーソナルコンピュータなどの情報処理装置１２０（図４参照）のデータファイル処理機能ｆ２２（図４参照）にデータおよび宛先を入力するが、このユーザが送信するデータに対して否認防止の判定結果を必要とする場合は、更に、否認防止要求を入力する。

【０１２５】

（１）ユーザが入力したデータはネットワーク通信管理部１０２０（図３参照）について説明したように、データファイル処理機能ｆ２２からネットワーク送受信管理機能ｆ１２に伝達されるが、「否認防止要求」はユーザセキュリティ機能ｆ２１を経由して通信管理セキュリティ機能ｆ１１に伝達される。通信管理セキュリティ機能ｆ１１では、否認防止要求８０１を受けてネットワーク送受信管理機能ｆ１２に伝達されたデータをもとに否認防止ファイル８０２を作成する。

【０１２６】

否認防止ファイル８０２は、ユーザが入力したデータに識別子を付加したもの、または、ユーザが入力したデータをハッシュ関数で処理したハッシュ値に識別子を付加したものである。

【０１２７】

ハッシュ関数は、「インターネットセキュリティ」オーム社、著者、佐々木良一、宝木和夫他のＰ９１に記載されているように、

▲１▼　一方向性　；あるハッシュ関数の出力値が与えられた場合、同じ出力値をもたらす別のメッセージＭを求めることが計算量的に困難であること。

【０１２８】

▲２▼　衝突回避性；同じハッシュ値となるような２つの異なるメッセージＭ１，Ｍ２を見つけることが、計算量的に困難であること。

【０１２９】

の特性をもったものである。

【０１３０】

（２）通信管理セキュリティ機能ｆ１１は、作成した否認防止ファイルを、鍵管理用ワークステーション１４０の否認防止管理機能ｆ４１に送付し、否認防止管理機能ｆ４１は、送付された否認防止ファイル８０２を識別子と対応させて否認防止管理データベース２６に格納する。

【０１３１】

（３）ネットワーク送受信管理機能ｆ１２に伝達したデータは、暗号化通信処理部１０３０（図３参照）を介して送信先相手ユーザ側のネットワーク送受信管理機能ｆ１２に伝達される。復号化されたデータは、そのまま送信先相手ユーザに伝達されるが、否認防止要求８０１がある場合、通信セキュリティ管理機能ｆ１１は、送達されたデータをもとに、発信側と同様に、否認防止ファイル８０３を作成し、鍵管理用ワークステーション１４０の否認防止管理機能ｆ４１に伝達する。

【０１３２】

否認防止管理機能ｆ４１は、受信側から送達された否認防止ファイル８０３を識別子と対応させて否認防止管理データベース２６に格納する。

【０１３３】

（４）否認防止管理機能ｆ４１は、送信側のユーザから送られた否認防止ファイル８０２と受信側のユーザから送られた否認防止ファイル８０３とを比較し、両者が一致する場合

否認防止が正常と判定し、一致しない場合は異常と判定し、この否認防止判定結果を否認防止管理データベース２６に登録する。

【０１３４】

（５）データの送受信が終了後、送信側または受信側のユーザが否認防止照会要求をデータファイル処理機能ｆ２２に入力すると、この要求は、ユーザセキュリティ機能ｆ２１、通信管理セキュリティ機能ｆ１１を経由して否認防止管理機能ｆ４１に送達される。否認防止管理機能ｆ４１は否認防止照会要求を受けると、否認防止管理データベース２６から否認防止判定結果を検索し、この結果を否認防止照会要求を入力したユーザに送付する。

【０１３５】

（６）否認防止ファイルとして、ハッシュ値を作成する場合は、ハッシュ値のデータ量が小さいため、鍵管理用ワークステーション１４０の否認防止管理機能ｆ４１ばかりでなく、送信先相手のユーザに送信するデータに付加して送付することも可能である。

【０１３６】

この場合、受信側の通信セキュリテイ機能ｆ１１は、受信したデータをもとにハッシュ値を算出し、送信側のユーザが送付したハッシュ値と比較することにより、否認防止を確認することができる。

【０１３７】

受信側の通信セキュリテイ機能ｆ１１で実施した否認防止の確認結果が異常で、送信側と受信側のユーザ間でトラブルが生じた場合、第三者的な立場である鍵管理用ワークステーション１４０に問い合わせることにより、どちらに否があるか判定することが可能となる。

【０１３８】

以下に、本発明を適用したネットワーク通信システムが提供する「鍵回復機能」の実施例について説明する。ここでは、暗号化通信を行う場合、図６に示すように、暗号に用いる鍵は二重の階層構造を有しているものとする。図６において、ユーザが送信するデータをＭとし、ネットワーク通信管理用ワークステーション１４０が生成するスクランブル鍵K_Sによりデータは暗号化され、暗号文E_{KS}（Ｍ）が作成される。この暗号文を復号するためのデスクランブル鍵K_Dを、鍵管理用ワークステーション１４０から送付されたセッション鍵P_Tによって暗号化し、暗号文E_{PT}（K_D）を作成している。

【０１３９】

鍵回復機能は、暗号文E_{KS}（Ｍ）に解読の情報を付加し、デスクランブル鍵K_Dによらずに暗号文を解読する手段を与えるものである。

【０１４０】

まず、図９を参照して、スクランブル鍵K_Sでデータを暗号化する際、鍵回復機能を持たせるための付加データの作成手順について説明する。

【０１４１】

（１）スクランブル鍵K_Sを生成するとき、乱数を生成しＫ１，Ｋ２の排他的論理和（ＸＯＲ、図では、直和記号で示している。）により、スクランブル鍵をK_S＝　Ｋ１　ＸＯＲ　Ｋ２と表現できるようにする。

【０１４２】

（２）Ｐ１，Ｐ２を鍵回復用の鍵とし、ネットワーク通信管理用ワークステーション１１０（図４参照）および、鍵管理用ワークステーション１４０（図４参照）の鍵回復機能ｆ４３（図４参照）で保管するものとする。スクランブル鍵K_Sを生成するときに生成したＫ１，Ｋ２をこの鍵回復用の鍵Ｐ１，Ｐ２で暗号化して暗号文E_{P1}（Ｋ１）、E_{P2}（Ｋ２）を作成する。このデータを、スクランブル鍵K_Sで作成したデータの暗号文E_{KS}（Ｍ）に付加するものとする。

【０１４３】

次に、図１０を参照して、この付加データで暗号文を復号する手順について説明する。

【０１４４】

（１）暗号文から付加されたデータE_{P1}（Ｋ１）、E_{P2}（Ｋ２）を分離し、鍵回復用の鍵

Ｐ１，Ｐ２でＫ１，Ｋ２を復号する。

【０１４５】

（２）Ｋ１，Ｋ２の排他的論理和を取り、K_S＝　Ｋ１　ＸＯＲ　Ｋ２として、スクランブル鍵K_Sを生成する。共通鍵暗号の場合、スクランブル鍵K_Sとデスクランブル鍵K_Dとは同一であり、このスクランブル鍵K_Sにより、暗号文を復号することができる。

【０１４６】

不測の事態が発生して、暗号文を解読する必要が生じた場合、暗号文を鍵管理用ワークステーション１４０（図４参照）に送付すれば、上記に示した手順により、鍵回復用の鍵Ｐ１，Ｐ２を用いて暗号文を解読することができる。

【０１４７】

以上で本ネットワーク通信システムを構成する６つの制御処理部のソフト機能の実施例について説明した。

【０１４８】

本ネットワーク通信システムにおいて、アクセス管理部によるユーザ認証は、ネットワーク通信管理用ワークステーションにより、このワークステーションと接続するユーザに対して実施される。即ち、ユーザ認証は複数のユーザで構成されるグループごとに実施される。また、ネットワーク通信管理部と暗号化通信処理部により、ネットワーク通信管理用ワークステーション間で暗号化通信が実施され、データを送信するユーザが暗号化し、これを受信するユーザが復号化するような、ユーザ対ユーザの暗号化通信は実施していない。

【０１４９】

このため、図１に示すネットワーク通信システムにおいて、ネットワーク通信管理用ワークステーションと、これと接続する複数のユーザで構成されるグループにおいて、１つの閉じたネットワークを構築することができる。

【０１５０】

次に、図１１を参照して、１つのグループに設置されたネットワーク管理ワークステーションごとに共通鍵暗号方式で、閉じたネットワークを構築する場合の鍵の階層構造について説明する。ここでは、Ｍ個所のグループにネットワーク通信管理用ワークステーション１１０＜１＞～１１０＜Ｍ＞を設置している。

【０１５１】

ネットワーク通信管理用ワークステーション１１０＜ｊ＞（$1 \leqq j \leqq M$）には、n_j個のユーザが使用するパーソナルコンピュータなどの情報処理装置が接続しネットワークを構成している。ユーザには、ユーザＩＤ、および、マスター鍵としての秘密鍵が割り当てられている。これらのユーザをユーザ１～ユーザn_jとし、ユーザｉ（$1 \leqq i \leqq n_j$）に割り当てられた秘密鍵をP_{ji}、ユーザＩＤをＩＤｊｉとする。ネットワーク通信管理ワークステーション１１０＜ｊ＞は、このユーザ１～ユーザn_jのマスター鍵としての秘密鍵を管理するため、ユーザＩＤデータベース１１にn_j個のユーザＩＤ｛ＩＤｊ１，ＩＤｊ２，…ＩＤｊｉ，…，ＩＤｊn_j｝を登録し、ユーザ鍵管理データベース１２にユーザマスター鍵としての秘密鍵とユーザＩＤを対応させたn_j個のデータ（ＩＤｊ１，Ｐｊ１），（ＩＤｊ２，Ｐｊ２）．．．（ＩＤｊｉ，Ｐｊｉ），．．．（ＩＤｊn_j，Ｐｊn_j）を登録している。ユーザ認証は、ユーザに割り当てられたマスター鍵としての秘密鍵により、図４に示す共通鍵によるユーザ認証方式に従って実施される。

【０１５２】

各ネットワーク通信管理用ワークステーション１１０＜ｊ＞には、ネットワークＩＤとしてSD_j、およびマスター鍵としての秘密鍵P_{Sj}が割り当てられており、鍵管理用ワークステーション１４０がこれらのネットワークＩＤと秘密鍵S_{Dj}を管理している。鍵管理用ワークステーション１４０のネットワークユーザＩＤデータベース２５には、ネットワーク管理用ワークステーション１１０＜ｊ＞のネットワークＩＤであるSD_jと、これが管理しているユーザのユーザＩＤ｛ID_{j1}，ID_{j2}，…，ID_{jnj}｝を対応させて登録している。さらに、ネットワーク鍵構成データベース２４には、ネットワークＩＤであるSD

$_j$と秘密鍵P_{Sj}を対応させて登録している。ネットワーク通信管理用ワークステーション１１０＜ｊ＞に属するユーザｉが暗号化通信を実施する場合、
（１）送信先相手ユーザの宛先（名前）および送信するデータＭを入力する。
【０１５３】
（２）ネットワーク通信管理用ワークステーション１１０＜ｊ＞は、鍵管理用ワークステーション１４０に暗号化通信を実施するためのセッション鍵発行の要求を行う。
【０１５４】
（３）鍵管理用ワークステーション１４０の鍵構成管理機能ｆ４１（図４参照）は、送信先相手ユーザの宛先（名前）をもとにネットワークユーザデータベース２５を検索する。送信先相手ユーザがネットワーク通信管理用ワークステーション１１０＜ｋ＞と接続するユーザであったとすると、相手ユーザのユーザＩＤであるID_{kl}および、相手ユーザが接続するネットワーク通信管理用ワークステーション１１０＜ｋ＞のネットワークＩＤであるSD_kを取得する。
【０１５５】
送信側ユーザが接続するネットワーク通信管理用ワークステーション１１０＜ｊ＞のネットワークＩＤはSD_jであり、相手先ユーザが接続するネットワーク通信管理用ワークステーション１１０＜ｋ＞のネットワークＩＤはSD_kである。
【０１５６】
このネットワークＩＤであるSD_j，SD_kをキーとして、ネットワーク鍵構成データベース２４を検索し、SD_jとSD_kとに対応する秘密鍵P_{Sj}，P_{Sk}を取得する。
【０１５７】
次に、セッション鍵P_Tを生成し、取得した秘密鍵で暗号化し、暗号化セッション鍵E_{PSj}（P_T），E_{PSk}（P_T）を作成する。
【０１５８】
（４）鍵管理用ワークステーション１４０は、暗号化セッション鍵E_{PSj}（P_T），E_{PSk}（P_T）と、送信先相手ユーザが接続しているネットワーク管理用ワークステーション１１０＜ｋ＞のネットワークＩＤであるSD_kとをセッション鍵発行要求元のネットワーク通信管理用ワークステーション１１０＜ｊ＞に発行する。
【０１５９】
（５）ネットワーク通信管理用ワークステーション１１０＜ｊ＞は、所有しているマスター鍵としての秘密鍵PS_jで暗号化セッション鍵E_{PSj}（P_T）を復号し、セッション鍵P_Tを取得する。
【０１６０】
次に、スクランブル鍵K_S、デスクランブル鍵K_Dを生成し、まず送信するデータＭを、スクランブル鍵K_Sで暗号化し、暗号文E_{KS}（Ｍ）を作成する。次にデスクランブル鍵K_Dを、セッション鍵P_Tで暗号化し、暗号化デスクランブル鍵E_{PT}（K_D）を作成する。
【０１６１】
一方、送付されたネットワークＩＤであるSD_kにより送信先相手をネットワーク通信管理用ワークステーション１１０＜ｋ＞と指定して接続し、作成した暗号文E_{KS}（Ｍ）、暗号化デスクランブル鍵E_{PT}（K_D）、および、送付された暗号化セッション鍵E_{Pk}（P_T）をデータとして合成して送付する。
【０１６２】
（６）上記暗号化されたデータを受信したネットワーク通信管理用ワークステーション１１０＜ｋ＞は、所有しているマスター鍵としての秘密鍵P_{sk}で暗号化セッション鍵E_{Psk}（P_T）を復号し、セッション鍵P_Tを取得する。
【０１６３】
次に、このセッション鍵より暗号化デスクランブル鍵E_{PT}（K_D）を復号し、デスクランブル鍵K_Dを取得する。このデスクランブル鍵K_Dにより暗号文E_{kS}（Ｍ）を復号し、データＭを取り出す。この復号して得られたデータＭを送信先相手のユーザＩＤがID_{kl}であるユーザに送付する。

【０１６４】
以上の手順で、ネットワーク管理用ワークステーション１１０＜ｊ＞に接続するユーザＩＤｊｉから、ネットワーク管理用ワークステーション１１０＜ｋ＞に接続するユーザＩＤｋｌに暗号化通信が実施される。
【０１６５】
本ネットワーク通信システムの鍵管理用ワークステーションは、各ネットワーク通信管理用ワークステーションに割り付けられたマスター鍵としての秘密鍵の管理は実施するものの、各ネットワーク通信管理用ワークステーションに接続するユーザに対しては、割り当てられたユーザＩＤは管理するものの、割り当てられたマスター鍵としての秘密鍵は管理していない。
【０１６６】
逆に、ユーザに対して割り当てられたマスター鍵としての秘密鍵を管理しているのは、このユーザと接続しているネットワーク通信管理用ワークステーションだけである。
【０１６７】
このことから、ネットワーク通信管理用ワークステーションと、これと接続しているユーザ間でひつのグループとして閉じたネットワークを構築していることがわかる。
【０１６８】
共通鍵暗号でシステムを構築する場合、各ユーザに割り当てられたマスター鍵としての秘密鍵は、ユーザ認証のみに用いられ、ネットワーク外部へは、暗号化通信に用いる鍵として使用されないため、このネットワーク通信管理用ワークステーションが設置されているグループは、ユーザ認証用として独自の暗号アルゴリズムを使用してもよい。
【０１６９】
セキュリティを確保するため、このグループのネットワーク内ユーザ間相互の暗号化通信を、ユーザに割り当てられたマスター鍵を使用して実施することも可能である。
【０１７０】
実施例として、ネットワーク管理用ワークステーションに属するユーザＩＤがＩＤｊｉであるユーザからユーザＩＤがＩＤｊｒであるユーザに暗号化通信を実施するものとすると、ネットワーク通信管理用ワークステーションは、セッション鍵Ｔを生成し、ＩＤｊｉに対応するマスター鍵としての秘密鍵ＰｉとＩＤｊｒに対応するマスター鍵としての秘密鍵Ｐｒでセッション鍵P_Tを暗号化し、暗号化セッション鍵E_{Pi}（Ｔ），E_{Pr}（Ｔ）を生成する。これをユーザＩＤがＩＤｊｉであるユーザに送付する。
【０１７１】
送信元のユーザは、マスター鍵としての秘密鍵P_iで暗号化セッション鍵E_{Pj}（Ｔ）を復号し、セッション鍵P_Tを取得する。
【０１７２】
このセッション鍵P_TによりデータＭを暗号化し、暗号文E_T（Ｍ）を作成し、送付された暗号化セッション鍵E_{Pr}（Ｔ）をこの暗号文に付加して送信する。この暗号文E_T（Ｍ）と暗号化セッション鍵E_{Pr}（Ｔ）を送付することで、ネットワーク内で暗号化通信を実施することが可能となる。
【０１７３】
この場合、グループに設置されたネットワーク通信管理用ワークステーションは、通信セキュリテイ管理機能において、グループのネットワーク内の暗号化通信に使用するセッション鍵を生成することになる。
【０１７４】
以上で、本発明のネットワーク通信システムを構成する６つの制御処理部のソフト機能の実施例を示した。図４に示すネットワーク通信システムに組み込まれるソフト機能において、暗号演算に関する処理は、ユーザセキュリティ機能、通信管理セキュリティ機能、スクランブル機能、デスクランブル機能で実施している。
【０１７５】
つぎに、図１２を参照して、このような暗号演算を実施する暗号処理装置をユーザが使用

するパーソナルコンピュータなどの情報処理装置、およびネットワーク通信管理用ワークステーションに組み込んだ実施例について説明する。

【０１７６】

ユーザが使用するパーソナルコンピュータ１２１は、ユーザが使用する情報処理装置の１つであり、ユーザが使用するＣＡＤ１２２（図２参照）でもよい。ユーザが使用するパーソナルコンピュータ１２１は、通常、ＣＰＵ２およびデータ処理装置３を内蔵しており、データファイル処理機能ｆ２２（図４参照）、ユーザセキュリティ機能ｆ２１（図４参照）に関する処理を行う。ネットワーク通信管理用ワークステーション４も、ＣＰＵ５およびデータ処理装置６を内蔵しており、ネットワーク送受信管理機能ｆ１２（図４参照）、通信セキュリティ管理機能ｆ１１（図４参照）、通信構成管理機能ｆ１５（図４参照）、スクランブル機能ｆ１３（図４参照）、デスクランブル機能ｆ１４（図４参照）に関する処理を行う。

【０１７７】

ユーザセキュリティ機能ｆ２１（図４参照）、および、通信管理セキュリティ機能ｆ１１（図４参照）によりアクセス管理部１０１０（図３参照）が行うユーザ認証のための暗号処理を、ユーザ認証用暗号装置７、８により実施している。

【０１７８】

ユーザ認証の過程で、ユーザは自分に割り当てられたマスター鍵を入力する。このマスター鍵はユーザが暗記して入力することも可能であるが、本実施例では、ＩＣカードにマスター鍵を記録させておきＩＣカード制御部９から入力している。

【０１７９】

ユーザが使用するパーソナルコンピュータ１２１とネットワーク管理用ワークステーション１１０とはＬＡＮ１０で接続されており、ネットワーク１１を構成している。ネットワーク管理用ワークステーション１１０と接続するユーザに割り当てられたマスター鍵は、ユーザ鍵管理データベース１２に登録され、ＩＣカードで入力されるユーザのマスター鍵を使用して暗号化通信を行い、ユーザ認証が行われる。

【０１８０】

ネットワーク通信管理用ワークステーション１１０と、これに属するユーザとはＬＡＮ１０で接続され、接続する全てのユーザに対して、このネットワーク通信管理用ワークステーションワークステーション１１０によるユーザ認証が実施される。このため、このグループで独立の閉じたネットワークを構成することができる。

【０１８１】

アクセス管理部１０１０（図３参照）によるユーザ認証が終了すると、ネットワーク通信管理用ワークステーション１１０間で暗号化通信処理部１０３０（図３参照）による暗号化通信が実施される。暗号化通信処理部１０３０（図３参照）により暗号化通信を行う場合、鍵管理用ワークステーション１４０（図４参照）から暗号化されたセッション鍵が送付される。ここでネットワーク通信管理ワークステーション１１０と接続するユーザ間で閉じたネットワークを構成するため、図１１の共通鍵暗号方式の鍵の階層構造で示すように、ネットワーク通信管理用ワークステーション１１０には、ネットワークマスター鍵を割り当てておくものとする。これより、送信側のネットワーク通信管理用ワークステーション１１０のネットワークマスター鍵をP_{Si}、受信側のネットワーク通信管理用ワークステーション１１０のネットワークマスター鍵をP_{Sj}とすると、鍵管理用ワークステーション１４０（図４参照）は、セッション鍵P_Tを生成し、これを上記ネットワークマスター鍵P_{Si}、P_{Sj}で暗号化し、暗号文$E_{PSi}（P_T）$、$E_{PSj}（P_T）$を送信する。

【０１８２】

図４に示すネットワーク通信システムに組み込むソフト機能のうち、まずスクランブル機能について説明する。

【０１８３】

図１２のセッション鍵復号化装置１３は、鍵管理用ワークステーションが送付した暗号化セッション鍵$E_{PSi}（P_T）$を送受信設備１４を経由して受信する。これをネットワーク通

信管理用ワークステーション１１０に割り当てられ、ユーザ鍵管理データベース１２に格納しているネットワークマスター鍵P_{Si}で復号演算を行い、セッション鍵P_Tを取得し、スクランブル鍵暗号化装置１５に引き渡す。スクランブル鍵、デスクランブル鍵生成装置１６は、データの暗号化に使用するスクランブル鍵K_Sおよび、データの復号化に使用するデスクランブル鍵K_Dを生成し、暗号処理管理装置１７に引き渡す。暗号処理管理装置１７は、スクランブル鍵K_Sをデータ暗号化装置１８に引き渡し、デスクランブル鍵K_Dをデスクランブル鍵暗号化装置１５に引き渡す。ユーザが入力したデータMは、ユーザが使用するパーソナルコンピュータ１のデータ処理装置３より入力され、データ暗号化装置１８へ伝達される。デスクランブル鍵暗号化装置１５は、セッション鍵復号化装置１３より送られたセッション鍵ＰＴによりデスクランブル鍵K_Dの暗号化を行い暗号文$E_{PT}（K_D）$を作成し、データ暗号化装置１８は、スクランブル鍵K_SによりデータMの暗号化を行い暗号文E_{KS}（M）を作成する。この暗号化の過程を暗号化処理管理装置１７が管理している。データの暗号化通信を実施する場合、データの暗号文E_{KS}（M）と暗号化デスクランブル鍵$E_T（K_D）$を同時に受信しても、まず、K_Dを復号化してからでないとE_{KS}（M）を復号化することができない。このように、暗号化デスクランブル鍵$E_{PT}（K_D）$は、暗号文E_{KS}（M）よりも先に受信し復号しておく必要がある。

【０１８４】

次に、図１３を参照して、共通鍵暗号でのスクランブル鍵の切り変えに、データの復号を円滑にするためのデスクランブル鍵配送シーケンスについて説明する。

【０１８５】

ユーザＡからユーザＢに暗号化通信を実施する場合、ある定まったデータ量が伝達されると、暗号化に使用するスクランブル鍵を新しく生成してスクランブル鍵の切り替えを実施し、暗号化通信のセキュリテイを確保するようにしている。図１３は、このスクランブル鍵の切り替えとデータの暗号化のシーケンスを示している。スクランブル鍵のｉ－１回目の切り替え時のデータをM_{i-1}，ｉ回目の切り替え時のデータをM_i，ｉ＋１回目の切り替え時のデータをM_{i+1}とする。

【０１８６】

（Ｓ１３０１）　データM_{i-1}を暗号化する場合、スクランブル鍵とデスクランブル鍵の生成を行うが、このときデータM_iを暗号化する時に使用するスクランブル鍵K_{Si}とデスクランブル鍵K_{Di}を生成し、一旦メモリに格納しておく。

【０１８７】

（Ｓ１３０２）　スクランブル鍵を切り替え、データM_iを暗号化する場合、データM_{i+1}を暗号化する時に使用するスクランブル鍵K_{Si+1}とデスクランブル鍵K_{Di+1}を生成し、一旦メモリに格納する。このメモリからデスクランブル鍵K_{Di}、K_{Di+1}を取り出し、セッション鍵ＰＴにより暗号化し、暗号文$E_{PT}（K_{Di}$、$K_{Di+1}）$を作成する。同様にメモリからスクランブル鍵K_{Si}を取り出し、データM_iを暗号化し暗号文$E_{KSi}（M_i）$を作成する。次に、作成した暗号文$E_{PT}（K_{Di}$、$K_{Di+1}）$、$E_{KSi}（M_i）$をペアとしてユーザＢに送付する。

【０１８８】

暗号文を送付後、使用したスクランブル鍵K_{Si}とデスクランブル鍵K_{Di}をメモリから消去する。

【０１８９】

ユーザＢはセッション鍵P_Tにより送付された暗号文$E_{PT}（K_{Di}$、$K_{Di+1}）$を復号化し、デスクランブル鍵K_{Di}、K_{Di+1}を取り出す。取り出したデスクランブル鍵K_{Di+1}を、メモリに格納し次に送付される暗号文を復号する準備をする。

【０１９０】

（Ｓ１３０３）　スクランブル鍵を切り替え、データM_{i+1}を暗号化する場合、データM_{i+2}を暗号化する時に使用するスクランブル鍵K_{Si+2}とデスクランブル鍵K_{Di+2}を生成し、一旦メモリに格納する。このメモリからデスクランブル鍵K_{Di+1}、K_{Di+2}を取り出し、セッション鍵P_Tにより暗号化し、暗号文$E_{PT}（K_{Di+1}$、$K_{Di+2}）$を作成する。同様にメモ

リからスクランブル鍵K_{Si+1}を取り出し、データM_{i+1}を暗号化し暗号文E_{KSi+1}（M_{i+1}）を作成する。次に、作成した暗号文E_{PT}（K_{Di+1}、K_{Di+2}）、E_{KSi+1}（M_{i+1}）をペアとしてユーザＢに送付する。

【０１９１】

（４）暗号文を送付されたユーザＢは、準備していたデスクランブル鍵K_{Di+1}により暗号文E_{KSi+1}（M_{i+1}）を復号化し、データM_{i+1}を取得する。データM_{i+1}を取得後使用したデスクランブル鍵K_{Di+1}をメモリから消去する。

【０１９２】

次に、セッション鍵P_Tにより送付された暗号文E_{PT}（K_{Di+1}、K_{Di+2}）を復号化し、デスクランブル鍵K_{Di+1}、K_{Di+2}を取り出す。取り出したデスクランブル鍵K_{Di+2}をメモリに格納し次に送付される暗号文を復号する準備をする。

【０１９３】

前述のデータＭｉ＋１の復号化がうまく行かなかった場合、取り出したデスクランブル鍵K_{Di+1}で再度復号化演算を試みるものとする。前述のデータM_{i+1}の復号化がうまく行っている時は、デスクランブル鍵K_{Di+1}は消去するものとする。

【０１９４】

以上のようなシーケンスにより、データの暗号文の送付と同時にデータの復号が可能となる。暗号処理管理装置１７（図１２参照）は、上記シーケンスでデスクランブル鍵の暗号文E_{PT}（K_{Di}、K_{Di+1}）および，データM_iの暗号文E_{KSi}（M_i）が作成されるように管理している。これらの暗号文が作成されると合成装置１９（図１２参照）に送付され、暗号文をデータファイルとして合成し、送受信設備１４（図１２参照）を経由して配信される。

【０１９５】

鍵管理用ワークステーションからは、相手先に送付するセッション鍵に関する暗号文E_{PSj}（P_T）が送られてくるが、この暗号文はそのまま合成装置１９（図１２参照）、送受信設備１４（図１２参照）を経由して相手先に配信される。

【０１９６】

次に、図１２を参照して、ネットワーク通信システムのソフト機能（図４参照）のうちのデスクランブル機能について説明する。

【０１９７】

（１）セッション鍵復号化装置１３は、送信側のネットワーク通信管理用ワークステーションが送付した暗号化セッション鍵E_{PSj}（P_T）を送受信設備１４を経由して受信する。これをネットワーク通信管理用ワークステーション１１０に割り当てられたネットワークマスター鍵P_{Sj}で復号化を行い、セッション鍵P_Tを取得し、デスクランブル鍵復号装置２０に引き渡す。

【０１９８】

（２）受信する暗号文のデータはスクランブル機能で示したように、デスクランブル鍵についての暗号文E_{PT}（K_{Di}、K_{Di+1}）とデータＭｉについての暗号文E_{KSi}（M_i）とで構成されている。このデータは送受信設備１４を経由して分配装置２１に送達される。

【０１９９】

ここで暗号化デスクランブル鍵E_{PT}（K_{Di}、K_{Di+1}）とデータの暗号文E_{KSi}（M_i）に分離し、デスクランブル鍵同期装置２２に引き渡され、暗号化デスクランブル鍵は、デスクランブル鍵復号化装置２０へ、データの暗号文はデータ復号化装置２３に引き渡される。

【０２００】

（３）デスクランブル鍵復号化装置２０は、セッション鍵復号化装置１３からセッション鍵P_Tが送付されており、このセッション鍵P_Tを用いて、デスクランブル鍵同期装置２２から送付された暗号化デスクランブル鍵E_{PT}（K_{Di}、K_{Di+1}）の復号化し、デスクランブル鍵K_{Di}、K_{Di+1}を取得する。デスクランブル鍵同期装置２２は、図１３に示すデスクランブル鍵の配送シーケンスに従ってデスクランブル鍵をデータ復号化装置２３に引き渡す。データ復号化装置２３は、送付されたデスクランブル鍵K_{Di}で送付された暗号文E_{KSi}

（M_i）を復号し、データM_iを取得する。取得したデータM_iは、送信先相手ユーザの使用するパーソナルコンピュータ１のデータ処理装置３に送付される。

【０２０１】

以上本発明のネットワーク通信システムを構成する６つの制御処理部について、共通鍵暗号を用いた場合のソフト機能構成の実施例について示した。

【０２０２】

次に、図１４を参照して、公開鍵暗号を用いた場合のソフト機能構成の実施例について説明する。図１４は、公開鍵暗号を用いた場合のアクセス管理部のソフト機能構成が示されている。

【０２０３】

公開鍵暗号アルゴリズムとしては、信学技報　ＴＥＣＮＩＣＡＬ　ＲＥＰＯＲＴ　ＯＦ　ＩＥＩＣＥ　ＩＳＥＣ９７－１５　（１９９７－０７）「楕円曲線を利用した高速暗号化法」　宝木和夫，車谷博之に記載された楕円曲線暗号を用いるものとし、この楕円曲線暗号の鍵の演算を記載するために必要な楕円曲線のベースポイントをＰとする。

【０２０４】

パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理局よりユーザＩＤ，マスター鍵としての秘密鍵d_{ID}および対応する公開鍵Q_{ID}（$=d_{ID}\cdot P$；・は、楕円曲線上の演算）が割り当てられている。

【０２０５】

ネットワーク通信管理用ワークステーションのユーザＩＤデータベースには、このワークステーションに接続しているユーザに割り当てられたユーザＩＤが登録され、ユーザ鍵管理データベースには、このワークステーションに接続しているユーザの公開鍵がユーザＩＤと対応させて登録されている。

【０２０６】

アクセス管理部では、ユーザが使用するパーソナルコンピュータなどの情報処理装置のユーザセキュリテイ機能とネットワーク通信管理用ワークステーションの通信セキュリテイ機能間の暗号化通信によって、ユーザ認証を実施する。以下、この実施例を示す。

【０２０７】

（１）ユーザが、本ネットワーク通信システムを利用する場合、ユーザが使用するパーソナルコンピュータなどの情報処理装置にアクセス要求を入力する。ユーザセキュリテイ機能は、「シーケンス番号」を付加しユーザ認証要求として通信セキュリテイ機能に送付する。

【０２０８】

（２）この要求を受けて、通信セキュリティ機能はユーザに割り当てられた「ユーザＩＤ」をキーとして、ユーザＩＤデータベースを検索し、「ユーザＩＤ」が該当すれば、時刻情報（「月」，「日」，「時」，「分」，「秒」）と乱数から構成されるチャレンジコードＣＡＣを生成し、ユーザセキュリティ機能に送付する。

【０２０９】

（３）ユーザは、フロッピーデイスクまたは、ＩＣカードにユーザに割り当てられたマスター鍵としての秘密鍵d_{ID}を保管しており、この電子媒体に記録されている鍵を入力する。このマスター鍵で送付されたチャレンジコードＣＡＣに署名作成演算を実施し、作成した署名データSd_{ID}（ＣＡＣ）を通信セキュリティ機能に送付する。

【０２１０】

（４）通信管理セキュリティ機能は、「ユーザＩＤ」をキーとしてユーザ鍵管理データベースを検索し、ユーザに割り当てられているマスター鍵としての秘密鍵d_{ID}に対応する公開鍵Q_{ID}を取り出し、送付された署名データSd_{ID}（ＣＡＣ）と生成したチャレンジコードＣＡＣをもとに署名検証演算を実施する。

【０２１１】

署名検証演算により、ユーザセキュリテイ機能で使用した秘密鍵d_{ID}と通信管理セキュリティ機能で使用した公開鍵Q_{ID}が楕円曲線上の演算（$Q_{ID}=d_{ID}\cdot P$；・は楕円曲線上の

演算）として対応し、かつ、チャレンジコードＣＡＣが通信経路の途中で改竄されなければ、ユーザを正当なユーザと判断することができ、認証判定結果を認証完了とする。逆に、上記暗号処理に使用する鍵が対応しなかったり、チャレンジコードＣＡＣが改竄された場合は、認証判定結果を認証エラーとする。そして、このようにして得られた認証判定結果をユーザセキュリテイ機能に返送する。

【０２１２】

（５）ユーザセキュリテイ機能は、認証判定結果がユーザ認証完了の場合、「シーケンス番号」を除いてユーザ認証結果としネットワーク通信管理部に伝達する。

【０２１３】

なお、図３におけるネットワーク通信管理部のソフト機能構成は、暗号アルゴリズムとして、共通鍵暗号、公開鍵暗号のどちらを使用した場合も同じである。

【０２１４】

次に、図１５を参照して、公開鍵暗号アルゴリズムを使用した場合の暗号化通信処理部のソフト機能構成の実施例について説明する。

【０２１５】

公開鍵暗号アルゴリズムとしては、アクセス管理部１０１０（図３参照）で用いた公開鍵暗号アルゴリズムと同様、楕円曲線暗号アルゴリズムを使用しており、鍵の演算に必要は楕円曲線のベースポイントをＰとしている。

【０２１６】

暗号化通信を実施する場合、ネットワーク通信管理用ワークステーション１１０のスクランブル機能ｆ１３は、ネットワーク送受信管理機能ｆ１２（図４参照）から送信されるデータを受け取る。

【０２１７】

次に、鍵管理用ワークステーション１４０の鍵構成管理機能ｆ４１からセッション鍵の発行を受け、この鍵をもとに受け取ったデータを暗号化し暗号文を作成し、送信先相手ユーザ側のネットワーク通信管理用ワークステーション１１０のデスクランブル機能ｆ１４に送信する。

【０２１８】

デスクランブル機能ｆ１４は、送付された暗号文を復号化し、データを取得する。

【０２１９】

暗号化通信処理部１０３０（図３参照）を運用する前提条件として、前述のアクセス管理部１０１０（図３参照）と同様、パーソナルコンピュータなどの情報処理装置を使用する各ユーザには、鍵管理局より、ユーザＩＤとマスター鍵として、秘密鍵d_{ID}と、この秘密鍵に対応する公開鍵Q_{ID}（＝Ｐ・d_{ID}；・は楕円曲線上の演算）とを割り当てられており、鍵管理用ワークステーション１４０のネットワーク鍵構成データベース２４に、ユーザに割り当てた公開鍵Q_{ID}をユーザＩＤと対応させて登録し管理している。同様にネットワーク通信管理用ワークステーション１１０には、このワークステーションと接続するすべてのユーザの公開鍵Q_{ID}をユーザＩＤと対応させて、ユーザ鍵管理データベース１２に登録し管理しているものとする。

【０２２０】

以下、この暗号化通信処理部の実施例を示す。

【０２２１】

（１）暗号化通信を実施する場合、暗号化通信要求が発生すると、鍵管理用ワークステーション１４０は、ネットワーク鍵構成データベース２４を検索し、ユーザの送信する相手先ユーザの公開鍵Q_{YID}を取得する。この公開鍵Q_{YID}をセッション鍵として発信側のユーザの接続するネットワーク通信管理用ワークステーション１１０に送付する。

【０２２２】

（２）発信側のユーザの接続するネットワーク通信管理用ワークステーション１１０では、送信するデータＭ１５０４を、ネットワーク送受信管理機能ｆ１２から受け取り、暗号化するためのスクランブル鍵K_S１５０１と復号するためのデスクランブル鍵K_D１５０２

を生成する。このスクランブル鍵K_S１５０１とデスクランブル鍵K_D１５０２とを運用する暗号アルゴリズムは共通鍵暗号アルゴリズムとする。

【０２２３】

次に、ユーザの入力するデータＭ１５０４をスクランブル鍵K_S１５０１で暗号化し、暗号文E_{KS}（Ｍ）１５０６を作成する。

【０２２４】

また、デスクランブル鍵K_D１５０２を送付されたセッション鍵としての公開鍵Q_{YID}１５０７で暗号化し、暗号化デスクランブル鍵E_{QYID}（K_D）１５０８を生成する。

【０２２５】

公開鍵暗号の場合、送付された鍵Q_{YID}１５０８はそのまま暗号化のための鍵として使用することができる。

【０２２６】

このようにして作成した２組の暗号文E_{KS}（Ｍ）１５０６とE_{QYID}（K_D）１５０８とを送信相手先のユーザが接続するネットワーク通信管理用ワークステーション１１０に送信する。

【０２２７】

（３）送信相手先のネットワーク通信管理用ワークステーション１１０は、ユーザ鍵管理データベース１２を検索し、管理しているユーザのマスター鍵としての秘密鍵D_{YID}１５１０を取得する。

【０２２８】

この取得した秘密鍵D_{YID}１５１０で、暗号化デスクランブル鍵E_{QYID}（K_D）１５０８を復号し、デスクランブル鍵K_D１５０３を取得する。次に、このデスクランブル鍵K_D１５０３を用いて、暗号文E_{KS}（Ｍ）１５０６を復号し、データＭ１５０５を得る。

【０２２９】

（４）取得したデータＭ１５０５は、ネットワーク送受信管理機能ｆ１２を経由して送信先相手ユーザに伝達される。

【０２３０】

以上の方式で、ユーザからユーザへの暗号化通信を実施する。

【０２３１】

スクランブル鍵K_S，デスクランブル鍵K_Dを運用する共通鍵暗号アルゴリズムとしてＣＳデジタル放送で実績のあるＭＵＬＴＩ２暗号アルゴリズムを用いる。

【０２３２】

マスター鍵，セッション鍵を運用する暗号アルゴリズムは、前述のように共通鍵暗号アルゴリズムとは異なる楕円曲線暗号アルゴリズムを用いており、これにより、二重暗号方式が構成され、セキュリティの向上が図られている。

【０２３３】

次に、本発明のネットワーク通信システムにおいて、公開鍵暗号として楕円曲線暗号を用いた場合の鍵管理部の実施例を示す。公開鍵暗号を用いた場合の鍵管理部のソフト機能は、図７に示す共通鍵暗号の場合のソフト機能と同じである。前述の公開鍵暗号アルゴリズムを使用した場合の暗号化処理部、およびアクセス管理部のソフト機能構成の実施例に示すように、各ユーザのマスター鍵は秘密鍵d_{ID}であり、この秘密鍵と楕円曲線上の演算で公開鍵Q_{ID}（＝d_{ID}・Ｐ；・は楕円曲線上の演算）が対応している。

【０２３４】

また、スクランブル鍵およびデスクランブル鍵の暗号アルゴリズムは、共通鍵暗号アルゴリズムとしてＭＵＬＴＩ２暗号アルゴリズムとしている。

【０２３５】

鍵管理部は、本ネットワーク通信システムを使用するすべてのユーザのマスター鍵に関する情報および、暗号化通信に関与するセッション鍵を管理している。

【０２３６】

以下、図７を参照して、この鍵管理部について説明する。

【０２３７】
（１）マスター鍵の管理
本ネットワーク通信システムを使用する全ユーザには、ユーザＩＤおよびこれと対応してマスター鍵としての秘密鍵d_{ID}および対応する公開鍵Q_{ID}が割り当てられており、
同様にネットワーク通信管理用ワークステーション１１０には、ネットワークＩＤおよびこれと対応して、マスター鍵としての秘密鍵D_S，対応する公開鍵Q_Sが割り当てられている。
【０２３８】
鍵管理用ワークステーション１４０のネットワーク鍵構成データベース２４には、全ユーザに上記ユーザＩＤと、このユーザに割り当てられた公開鍵とを対応させ、また、全ネットワーク通信管理用ワークステーション１１０に上記ネットワークＩＤと、このワークステーションに割り当てられた公開鍵とを対応させて登録している。
【０２３９】
同じようにして、ネットワーク通信管理用ワークステーション１１０のユーザ鍵管理データベース１２には、このワークステーション１１０に割り当てられた上記ネットワークＩＤと対応して、マスター鍵としての秘密鍵D_S，対応する公開鍵Q_Sとを登録するとともに、このワークステーション１１０と接続するすべてのユーザのユーザＩＤとマスター鍵である秘密鍵d_{ID}および対となる公開鍵であるQ_{ID}とを対応して登録している。公開鍵暗号を用いる場合、ネットワーク鍵構成データベース２４は、公開鍵のみを登録し、秘密鍵を登録する必要がない。
【０２４０】
上記ユーザのマスター鍵としての秘密鍵および対となる公開鍵は、ネットワーク通信管理用ワークステーション１１０の通信構成管理機能ｆ１５と、鍵管理用ワークステーション１４０の鍵構成管理機能ｆ４１とによって管理されており、このユーザのマスター鍵の登録，更新，削除はこれらの機能のより実施される。
【０２４１】
ネットワーク通信管理用ワークステーション１１０設置時に、このワークステーション１１０のネットワークＩＤと、秘密鍵および対応する公開鍵を鍵管理用ワークステーション１４０の鍵構成管理機能ｆ４１が生成し、ネットワークＩＤデータベース２７およびネットワーク鍵構成データベース２４に登録するとともに、ネットワーク通信管理用ワークステーション１１０の通信構成管理機能ｆ１５により、ユーザＩＤデータベース２８およびユーザ鍵管理データベース１２に登録する。
【０２４２】
各ユーザの秘密鍵および対となる公開鍵も、鍵構成管理機能ｆ４１が生成し、公開鍵とユーザＩＤとを対応させてネットワーク鍵構成データベース２４に登録する。生成した各ユーザの秘密鍵および対となる公開鍵は、ユーザ鍵管理データベース１２に登録する必要があるが、上記ネットワーク通信管理用ワークステーション１１０設置時、通信構成管理機能ｆ１５より直接入力し登録することもできるが、ネットワーク通信用ワークステーション１１０に割り当てられた公開鍵を使用し、スクランブル機能ｆ１４により暗号化して配送することも可能である。
【０２４３】
同様に、ユーザのマスター鍵および、ネットワーク通信管理用ワークステーション１１０のマスター鍵の更新、削除に関するデータも上記ネットワーク通信管理用ワークステーション１１０に割り当てた公開鍵を使用し、スクランブル機能ｆ１４で暗号化して配送することもできる。
【０２４４】
鍵情報は、本ネットワーク通信システムにおいて、暗号化通信の根幹となる情報であるため、その正当性をネットワーク通信管理用ワークステーション１１０で確認する必要がある。このため、鍵管理用ワークステーション１４０には、固有のマスター鍵である秘密鍵d_Cおよび対応する公開鍵であるQ_C（$=d_C \cdot P$）を定め、送付する鍵情報に、鍵管理用

ワークステーションによる署名作成演算（電子署名）を実施する。
【０２４５】
当然、この公開鍵は、ネットワーク通信管理用ワークステーション１１０へ公開しておく。
【０２４６】
次に、上記マスター鍵の管理の手順について説明する。鍵構成管理機能１４０の生成するユーザの鍵に関する情報をＭとする。ここでは、鍵を更新する場合について示す。
【０２４７】
（ｉ）Ｍは、更新するユーザのユーザＩＤ，更新する秘密鍵d_{ID}，公開鍵Q_{ID}および更新日時で構成される。
【０２４８】
全てのネットワーク構成管理データベース２４を検索し、得られたユーザと接続するネットワーク通信管理用ワークステーション１１０のネットワークＩＤをI_S，公開鍵Q_Sとする。この公開鍵Q_Sには、鍵管理用ワークステーション４０による署名作成演算を実行して配布し、使用する側は署名検証演算により公開鍵Q_Sの正当性を確認するものとする。
【０２４９】
鍵情報を暗号化するためスクランブル機能が生成したスクランブル鍵をK_S，デスクランブル鍵をK_Dとする。
【０２５０】
（ｉｉ）鍵情報Ｍをスクランブル鍵K_Sで暗号化し、暗号文E_{KS}（Ｍ）を作成する。
【０２５１】
デスクランブル鍵K_Dを公開鍵Q_Sで暗号化し、暗号化デスクランブル鍵E_{QS}（K_D）を作成する。
【０２５２】
また、鍵情報Ｍに対して、鍵管理用ワークステーション１４０のマスター鍵である秘密鍵d_Cで署名作成演算を実施し署名データS_{dC}（Ｍ）を作成する。
【０２５３】
次に、このE_{KS}（Ｍ），E_{QS}（ＫＤ），S_{dC}（Ｍ）をネットワークＩＤであるI_Sで宛先を指定し、送信する。
【０２５４】
（ｉｉｉ）受信側のネットワーク管理用ワークステーション１１０は、デスクランブル機能ｆ１４にE_{KS}（Ｍ），E_{QS}（ＫＤ），S_{dC}（Ｍ）を送付する。デスクランブル機能ｆ１４は、ネットワーク通信管理用ワークステーション１１０に割り当てられた秘密鍵d_SによりE_{QS}（K_D）を復号し、デスクランブル鍵K_Dを取得する。
【０２５５】
次に、K_DによりE_{KS}（Ｍ）を復号し、鍵に関する情報Ｍを取得する。
【０２５６】
（ｉＶ）鍵に関する情報Ｍ、と鍵管理用ワークステーション１４０の公開鍵Q_Cとを用いて署名データS_{dC}（Ｍ）に対し署名検証演算を実施し、鍵に関する情報Ｍが正当な鍵管理用ワークステーション１４０から送付されたものであることを確認する。
【０２５７】
この確認が得られたら鍵情報Ｍを、通信構成管理機能ｆ１５に送り、この鍵情報Ｍをもとにユーザ鍵管理データベース１２を更新する。
【０２５８】
（Ｖ）各ユーザへのマスター鍵の更新、および配布は、ネットワーク通信管理用ワークステーション１１０側でＩＣカードまたはフロピーデイスクなどの記録媒体に記録してオフラインで配布するか、変更前のユーザに割り当てられた公開鍵で暗号化し、ネットワークを利用してオンラインで送付するころができる。これらのうち、どちらの方式をとるかは、状況によって定める。
【０２５９】

（２）セッション鍵の管理
（ｉ）暗号化通信処理部１０３０（図３参照）で暗号化通信を行う場合、発信側ユーザのネットワーク通信管理用ワークステーション１１０の通信セキュリティ管理機能ｆ１１から、発信側のユーザＩＤと送信先相手のユーザＩＤを付加したセッション鍵発行要求が、鍵管理ワークステーション１４０の鍵構成管理機能ｆ４１に送付される。
【０２６０】
（ｉｉ）鍵構成管理機能ｆ４１は、ユーザＩＤをキーとしてネットワーク鍵構成データベース２４を検索し、送信先相手ユーザのマスター鍵に対応する公開鍵Q_{YID}を取り出す。
【０２６１】
取り出した公開鍵Q_{YID}に対して、鍵管理用ワークステーション１４０のマスター鍵である秘密鍵d_Cで署名作成演算を実施し署名データS_{dC}（Q_{YID}）を作成する。
【０２６２】
この公開鍵Q_{YID}と署名データS_{dC}（Q_{YID}）とを、発信側ユーザのネットワーク通信管理用ワークステーション１１０の通信セキュリティ管理機能ｆ１１に発行する。
【０２６３】
（ｉｉｉ）公開鍵Q_{YID}と署名データS_{dC}（Q_{YID}）とを受信した通信セキュリティ管理機能ｆ１１は、鍵管理用ワークステーション１４０の公開鍵Q_Cを用いて署名データS_{dC}（Q_{YID}）対し署名検証演算を実施し、公開鍵Q_{YID}が正当な鍵管理用ワークステーション１４０から送付されたものであることを確認する。
【０２６４】
公開鍵Q_{YID}は、セッション鍵として、デスクランブル鍵を暗号化するために使用する。
【０２６５】
このようにして、セッション鍵が発行される。
【０２６６】
次に、本発明のネットワーク通信システムにおいて、公開鍵暗号として楕円曲線暗号を用いた場合の否認防止部のソフト機能について説明する。
【０２６７】
公開鍵暗号を用いた場合の否認防止部のソフト機能は、図８に示される、共通鍵暗号を用いた場合のソフト機能と同じであり、共通鍵暗号と同様、ユーザが否認防止要求を入力した場合、ネットワーク通信管理用ワークステーションの通信管理セキュリティ機能において、送信するデータをもとに否認防止ファイルの作成を行う。
【０２６８】
公開鍵暗号の場合、この否認防止ファイルは送信するデータに署名作成演算を実施したものを用い、鍵管理ワークステーションの否認防止機能は、第三者的な立場で否認防止の判定を行う。
【０２６９】
以下、図８を参照して、公開鍵暗号として楕円曲線暗号を用いた場合の否認防止部のソフト機能構成の実施例について説明する。
【０２７０】
（１）ユーザ（がネットワークアクセスに用いる情報処理装置１２０）がデータＭを送信するものとし、このユーザ１２０と接続するネットワーク通信管理用ワークステーション１１０に割り当てられた、ネットワークＩＤをI_S，これに対応する秘密鍵をd_S，公開鍵をQ_Sとする。
【０２７１】
ユーザが否認防止を必要とする場合は、データＭを入力するに際し否認防止要求８０１を入力する。
【０２７２】
（２）通信管理セキュリティ機能ｆ１１は、データＭには、ハッシュ関数と秘密鍵d_Sにより署名作成演算を実施し、署名データS_{dS}（Ｍ）を作成する。
【０２７３】

これに、ネットワークＩＤであるI_S、および、公開鍵Q_Sを付加して、否認防止ファイル８０２を作成する。通信管理セキュリティ機能は、作成した否認防止ファイル８０２を、鍵管理用ワークステーション１４０の否認防止管理機能ｆ４１および送信相手先のネットワーク送受信管理機能ｆ１２に送付する。

【０２７４】

（３）送信相手先の通信管理セキュリティ機能ｆ１１は、受信し復号して得られたたデータをハッシュ関数で処理したハッシュ値に識別子を付加し、これを鍵管理用ワークステーション１４０の否認防止機能ｆ４１に送付する。

【０２７５】

（４）鍵管理用ワークステーション１４０の否認防止機能ｆ４１は、送付された否認防止ファイル８０２および識別子の付加されたハッシュ値を、通信データの証拠として否認防止データベース２６に登録し、一方、送付された署名データS_{dS}（Ｍ）、付加された公開鍵Q_S，およびハッシュ値Ｅをもとに署名検証演算を実施し、この否認防止判定結果も、否認防止データベース２６に登録する。

【０２７６】

（５）受信側のネットワーク通信管理用ワークステーション１１０も同様に、受信したデータと、署名データS_{dS}（Ｍ）および付加されて送付された公開鍵Q_Sとにより署名検演算を実施し、否認防止の確認を行う。

【０２７７】

否認防止結果については、送信側のユーザにも伝達する。

【０２７８】

（６）受信側で実施した否認防止の確認結果についてトラブルが生じた場合、第三者的な立場の鍵管理用ワークステーション１４０に否認防止照会要求を行う。

【０２７９】

否認防止管理機能ｆ４１は、否認防止照会要求を受けると、否認防止管理データベース２６から否認防止判定結果を検索し、照会要求元に送付する。

【０２８０】

次に、本発明のネットワーク通信システムにおいて、公開鍵暗号として楕円曲線暗号を用いた場合の鍵回復部のソフト機能の実施例について説明する。

【０２８１】

図１５の公開鍵暗号アルゴリズムによる暗号化通信処理部で示すように、データＭの暗号化に用いるスクランブル鍵をK_S，デスクランブル鍵をK_Dとし、デスクランブル鍵を配送するためのセッション鍵としての公開鍵をQ_{YID}とすると、暗号化通信は、暗号文E_{KS}（Ｍ）と暗号化デスクランブル鍵E_{QYID}（K_D）の送信により実施される。

【０２８２】

まず、信学技報　ＴＥＣＮＩＣＡＬ　ＲＥＰＯＲＴ　ＯＦ　ＩＥＩＣＥ　ＩＳＥＣ９７－１５（１９９７－０７）に「楕円曲線を利用した高速暗号化方法」　宝木和夫，車谷博之に従って、暗号化デスクランブル鍵E_{QYID}（K_D）にしきい値ロジックを付加する鍵回復方式の実施例について説明する。

【０２８３】

（１）鍵管理用ワークステーション１４０（図４参照）の鍵回復機能ｆ４３（図４参照）において、鍵回復用の公開鍵Q_A，Q_B，Q_Cを割り当て、公開するとともに、この公開鍵に対応する秘密鍵d_A，d_B，d_C（$Q_A = d_A \cdot P$，$Q_B = d_B \cdot P$，$Q_C = d_C \cdot P$）を保管するものとする。

【０２８４】

暗号化デスクランブル鍵E_{QYID}（K_D）には、鍵Q_{YID}，Q_A，Q_B，Q_Cで算出されるしきい値ロジックを付加するものとする。

【０２８５】

（２）共通鍵暗号を用いた場合と同様、暗号化通信を行う場合、デスクランブル鍵K_Dを暗号化してからでないと、データをスクランブル鍵K_Sで暗号化できないようにし、デー

タの暗号文E_{KS}（M）と暗号化デスクランブル鍵E_{QYID}（K_D）は必ずペアで生成されるようにする。

【０２８６】

（３）不測の事態が発生して暗号文を解読する必要が生じた場合、ペアとなった暗号文E_{KS}（M），E_{QYID}（K_D）を鍵管理ワークステーション１４０（図４参照）に送付する。

【０２８７】

鍵回復機能ｆ４３（図４参照）では、秘密鍵d_A，d_B，d_Cの２つと、E_{QYID}（K_D）に付加されたしきい値ロジックを用いて復号し、デスクランブル鍵K_Dを取得する。

【０２８８】

次に、この鍵K_Dで暗号文E_{KS}（M）を復号し、データMを取得する。

【０２８９】

本発明のネットワーク通信システムでは、送信するデータMの暗号文は、スクランブル鍵K_Sによる暗号化演算で作成される。

【０２９０】

このため、共通鍵暗号を用いた鍵回復部（図９、図１０参照）と全く同様に、スクランブル鍵K_SをＫ１，Ｋ２の排他的論理和で表現し、これを用いて鍵回復を実施する方法をとることもできる。図９、１０に示す鍵回復用の鍵Ｐ１，Ｐ２は、共通鍵暗号アルゴリズムで運用することもできるが、鍵回復用として、公開鍵Q_A，Q_Bにより運用することも可能である。

【０２９１】

この場合暗号文E_{KS}（M）に鍵回復用として付加するデータは、Ｋ１，Ｋ２を公開鍵Q_A，Q_Bにより暗号化した暗号文E_{QA}（Ｋ１），E_{QB}（Ｋ２）であり、鍵回復は、鍵管理用ワークステーション１４０（図４参照）の鍵回復機能ｆ４３（図４参照）において公開鍵Q_A，Q_Bに対応する秘密鍵d_A，d_Bを用いて、付加されたデータを復号することにより実施する。

【０２９２】

暗号処理装置１７（図１２参照）において公開鍵暗号を使用した場合における、暗号処理管理装置１７（図１２参照）、デスクランブル鍵同期装置２２（図１２参照）を運用するシーケンスは、公開鍵暗号でのスクランブル鍵の切り替えのシーケンスは、図１６に示すようになる。

【０２９３】

なお、公開鍵暗号を使用した場合、公開鍵はそのままセッション鍵として使用されるため、図１２に描かれるセッション鍵復号化装置１３は不要となる。ただし、セッション鍵署名検証装置を設置し、鍵管理用ワークステーションが実施した署名作成演算を検証し、セッション鍵の正当性を確認するものとする。

【０２９４】

本発明のネットワーク通信システムでは、公開鍵暗号を用いた場合も共通鍵暗号を用いた場合と同様、ネットワーク通信管理用ワークステーションとこれと接続するユーザ（ユーザ用パーソナルコンピュータ）間で、１つの閉じたネットワークを構築することができる。

【０２９５】

次に、図１７を参照して、各情報の拠点に設置されたネットワーク管理用ワークステーションごとに、閉じたネットワークを構成する場合、公開鍵暗号を用いた鍵階層構造の実施例について説明する。

【０２９６】

この場合も、ネットワーク通信管理用ワークステーション１１０＜ｊ＞にn_j個のユーザが使用するパーソナルコンピュータが接続し、ネットワークを構成するものとする。

【０２９７】

ユーザｊのユーザＩＤをＩＤｊｉ，割り当てられた秘密鍵をD_{ji}，対応する公開鍵をQ_{ji}（＝d_{ji}・Ｐ）とする。

【０２９８】
ネットワーク通信管理用ワークステーション１１０＜ｊ＞は、ユーザＩＤデータベースにn_j個のユーザＩＤ｛ＩＤｊ１，ＩＤｊ２，…，$ＩＤｊn_j$｝を登録し、ユーザ鍵管理データベースには、ユーザＩＤとユーザの公開鍵を対応させたn_j個のデータ｛（ＩＤｊ１，Ｑｊ１），（ＩＤｊ２，Ｑｊ２），…，（ＩＤｊｉ，Ｑｊｉ），…，（$ＩＤｊn_j$，$Ｑｊn_j$）｝を登録している。
【０２９９】
ユーザ認証は、このネットワーク内で、図１２に示す公開鍵暗号アルゴリズムによるユーザ認証方式で実施される。
【０３００】
各ネットワーク通信管理用ワークステーション１１０＜ｊ＞には、ネットワークＩＤとして$Ｉ_{Sj}$、秘密鍵$ｄ_{Sj}$、および、これと対となる公開鍵$Ｑ_{Sj}$（＝$ｄ_{Sj}$・Ｐ）が割り当てられており、鍵管理用ワークステーション１４０は、ネットワークユーザＩＤデータベース２５に、ネットワーク管理用ワークステーション１１０＜ｊ＞のネットワークＩＤである$Ｉ_{Sj}$と、これが管理しているユーザのユーザＩＤ｛ＩＤｊ１，ＩＤｊ２，…，$ＩＤｊn_j$｝とを対応させて登録し、ネットワーク鍵構成データベース２４には、ネットワークＩＤである$Ｉ_{Sj}$と、ネットワーク通信管理用ワークステーション１１０＜ｊ＞の公開鍵$Ｑ_{Sj}$とを対応させた、ｍ個のデータ｛（$Ｉ_{S1}$，$Ｑ_{S1}$），（$Ｉ_{S2}$，$Ｑ_{S2}$），…，（$Ｉ_{Sm}$，$Ｑ_{Sm}$）｝を登録している。ネットワーク通信管理用ワークステーション１１０＜ｊ＞に属するユーザｉが、暗号化通信を実施する手順も、共通鍵暗号アルゴリズムを用いた場合とほぼ同様である。
【０３０１】
（１）ユーザｉが、送信相手の宛先（名前）および送信するデータＭを入力する。
【０３０２】
（２）ネットワーク通信管理用ワークステーション１１０＜ｊ＞は、鍵管理用ワークステーション１４０にセッション鍵発行要求を行う。
【０３０３】
（３）鍵管理用ワークステーション１４０の鍵構成管理機能ｆ４１（図４参照）は、ネットワークユーザＩＤデータベース２５を検索し、送信相手の宛先（名前）から相手ユーザのユーザＩＤとして$ＩＤ_{kl}$および相手ユーザが接続するネットワーク通信管理用ワークステーション１１０＜ｋ＞のネットワークＩＤとしての$Ｉ_{Sk}$を取得する。
【０３０４】
次に、このネットワークＩＤである$Ｉ_{Sk}$をキーとしてネットワーク鍵構成データベース２４を検索し、$Ｉ_{Sk}$に対する公開鍵$Ｑ_{Sk}$を取得する。
【０３０５】
（５）鍵管理用ワークステーション１４０は、セッション鍵としての$Ｑ_{Sk}$と送信相手先のネットワーク管理用ワークステーション１１０＜ｋ＞のネットワークＩＤである$Ｉ_{Sk}$とを、要求元のネットワーク通信管理用ワークステーション１１０＜ｊ＞に発行する。
【０３０６】
（６）ネットワーク通信管理用ワークステーション１１０＜ｊ＞は、セッション鍵$Ｑ_{Sk}$の発行を受け、スクランブル鍵$Ｋ_S$およびデスクランブル鍵$Ｋ_D$を生成する。
【０３０７】
次に、データＭをスクランブル鍵$Ｋ_S$で暗号化し、暗号文$Ｅ_{KS}$（Ｍ）を作成する。また、デスクランブル鍵$Ｋ_D$をセッション鍵$Ｑ_{Sk}$で暗号化し、暗号化デスクランブル鍵$Ｅ_{QSk}$（$Ｋ_D$）を作成する。そこで、ネットワークＩＤである$Ｉ_{Sk}$をもとに、送信の相手先と通信系を接続し、作成した暗号文$Ｅ_{KS}$（Ｍ），暗号化デスクランブル鍵$Ｅ_{QSk}$（$Ｋ_D$）を合成して送付する。
【０３０８】
（７）受信した相手先のネットワーク通信管理用ワークステーション１１０＜ｋ＞は、割り当てられているマスター鍵としての秘密鍵$ｄ_{Sk}$で暗号化デスクランブル鍵$Ｅ_{QSk}$（$Ｋ_D$）

を復号し、デスクランブル鍵K_Dを取得する。そして、このデスクランブル鍵K_Dにより暗号文E_{KS}（Ｍ）を復号し、データＭを取得する。

【０３０９】

次に、この復号したデータＭを送信相手先のユーザが使用するパーソナルコンピュータなどの情報処理装置１２０に送付する。

【０３１０】

以上の手順で、ネットワーク管理用ワークステーション１１０＜ｊ＞に接続するユーザＩＤがＩＤｊｉのユーザから、ネットワーク管理用ワークステーション１１０＜ｋ＞に接続するユーザＩＤがＩＤｋｌのユーザへの、暗号化通信が実施される。

【０３１１】

本実施例で示すように、本ネットワーク通信システムの鍵管理用ワークステーションは、各ネットワーク通信管理用ワークステーションに割り付けられた公開鍵を管理し、各ユーザに割り付けられた公開鍵は、このユーザと接続しているネットワーク通信管理用ワークステーションで管理している。

【０３１２】

ユーザ認証もこの鍵構成で実施でき、このことから、ネットワーク通信管理用ワークステーションとこれと接続しているユーザ間で１つの閉じたネットワークを構築していることがわかる。

【０３１３】

各ユーザに割り当てられた秘密鍵と公開鍵は、ユーザ認証のみに用いられ、ネットワーク外部への暗号化通信に用いる鍵としては使用されないため、このネットワーク内では、独自の方式の暗号アルゴリズムを使用することも可能である。

【０３１４】

この各ユーザに割り当てられた公開鍵でこのネットワーク内における暗号化通信を実施して、セキュリティを向上させることも可能である。

【０３１５】

上記ネットワーク内においてユーザＩＤがＩＤｊｉであるユーザからＩＤｊｒであるユーザに暗号化通信を実施する手順を以下に示す。

【０３１６】

（１）ユーザは、ＩＤｊｉからユーザＩＤｊｒへ暗号化通信を実施するためのセッション鍵の発行要求を接続するネットワーク通信管理用ワークステーション１１０＜ｊ＞に送付する。

【０３１７】

（２）ネットワーク通信管理用ワークステーション１１０＜ｊ＞は、ユーザ固有鍵データベースを検索し、ユーザＩＤｊｒに割り当てられた公開鍵Ｑｊｒを取得し、ユーザＩＤｊｒに送付する。

【０３１８】

（３）ユーザＩＤｊｉは公開鍵Ｑｊｒにより送付するデータＭを暗号化し、暗号文E_{Qr}（Ｍ）を作成し、ユーザＩＤｊｒに送付する。

【０３１９】

（４）暗号文E_{Qr}（Ｍ）を受信したユーザＩＤｊｒは、このユーザに割り当てられた公開鍵Ｑｊｒに対応する秘密鍵d_{jr}（$Q_{j}r = d_{jr} \cdot P$）を用いて暗号文を復号し、データＭを取得する。

【０３２０】

【発明の効果】

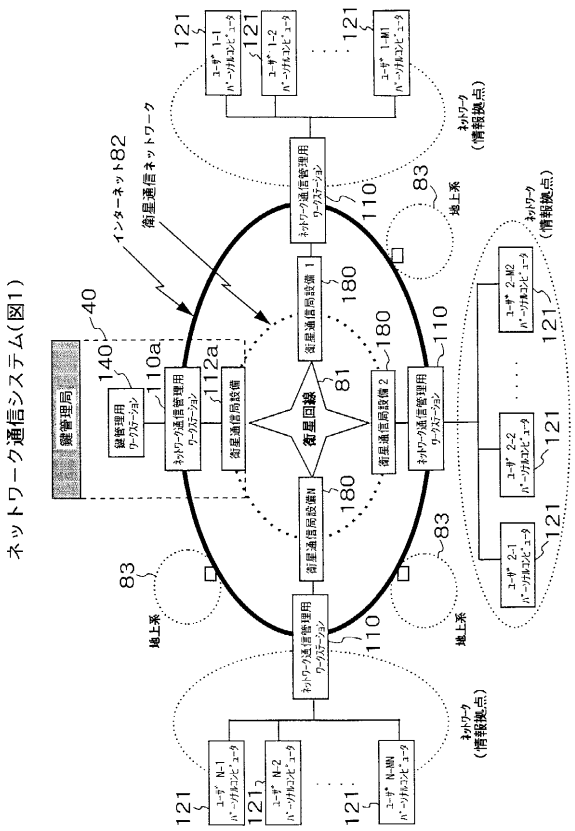
本発明によれば、複数のユーザで構成されるグループ群を双方向の通信ネットワークで結び、グループ間で構築した通信経路を利用して、各ユーザ間で情報を双方向に伝達するシステムにおいて、伝達する情報が変造，偽造，遺漏，不到達などの情報障害を受けないよう、安全性（セキュリティ）を確保することが可能となる。

【図面の簡単な説明】

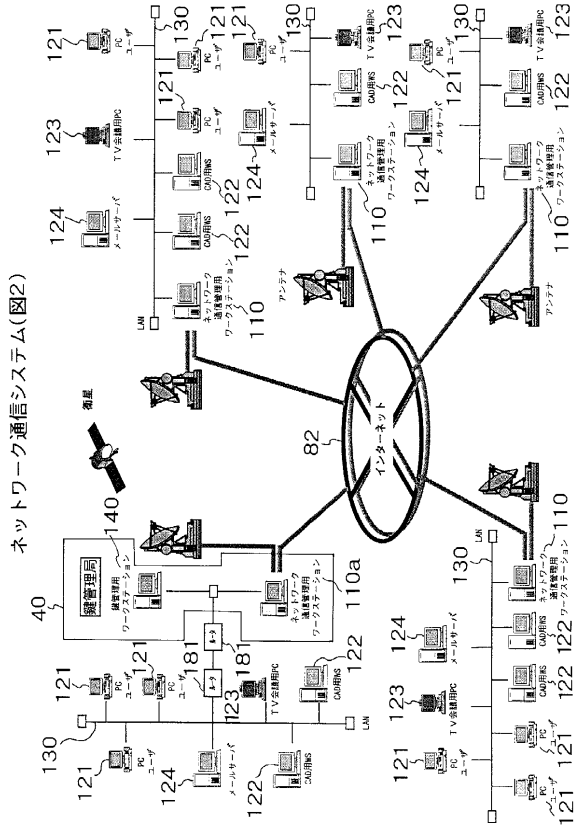
【図１】　本発明を適用したネットワーク通信システムを示すネットワーク構成図である。
【図２】　本発明を適用したネットワーク通信システムを示すシステム構成図である。
【図３】　本発明を適用したネットワーク通信システムを示すブロック構成図である。
【図４】　本発明を適用したネットワーク通信システムの各ブロックにおけるソフト機能を示す機能ブロック図である。
【図５】　共通鍵暗号アルゴリズムを用いたアクセス管理部のソフト機能構成を示す説明図である。
【図６】　共通鍵暗号アルゴリズムを用いた暗号化通信処理部を示す説明図である。
【図７】　鍵管理部を示す説明図である。
【図８】　否認防止部を示す説明図である。
【図９】　鍵復号部における暗号化の処理を示すフロー図である。
【図１０】　鍵復号部における復号化の処理を示すフロー図である。
【図１１】　共通鍵暗号方式を適用した場合の階層構造を示す説明図である。
【図１２】　本発明を適用したネットワーク通信システムの暗号処理装置を示すブロック図である。
【図１３】　共通鍵暗号方式を用いたスクランブル鍵の切り替え処理を示すフロー図である。
【図１４】　公開鍵暗号アルゴリズムを用いたアクセス管理部のソフト構成を示す説明図である。
【図１５】　公開鍵暗号アルゴリズムを用いた暗号化通信処理部を示す説明図である。
【図１６】　公開鍵暗号方式を用いたスクランブル鍵の切り替え処理を示すフロー図である。
【図１７】　公開鍵暗号方式の鍵の階層構造を示す説明図である。
【符号の説明】
１…パーソナルコンピュータ、２…ＣＰＵ、３…データ処理装置、５…ＣＰＵ、６…データ処理装置、８…ユーザ認証用暗号装置、７…ユーザ認証用暗号装置、９…ＩＣカード制御部、１１…ユーザＩＤデータベース、１２…ユーザ鍵管理データベース、１３…セッション鍵復号化装置、１５…デスクランブル鍵暗号化装置、１６…スクランブル鍵／デスクランブル鍵生成装置、１７…暗号処理管理装置、１８…データ暗号化装置、１９…合成装置、２０…デスクランブル鍵復号化装置、２２…デスクランブル鍵同期装置、２１…分配装置、２３…データ復号化装置、２４…ネットワーク鍵構成データベース、２５…ネットワークユーザＩＤデータベース、２６…否認防止管理データベース、２７…ネットワークＩＤデータベース、２８…ユーザＩＤデータベース、４０…鍵管理局、８１…衛星回線、８２…インターネット、８３…地上回線、１１０＜１＞～＜Ｎ＞，１１０ａ，１１０…ネットワーク通信管理用ワークステーション、１２０＜１－１＞～＜１－Ｍ１＞～＜Ｎ－ＭＮ＞，１２０…情報処理装置、１２１…パーソナルコンピュータ、１２２…ＣＡＤ用ワークステーション、１２３…ＴＶ会議用パーソナルコンピュータ、１２４…メールサーバ、１３０…ローカルエリアネットワーク、１８０…衛星通信局設備、１８１…ルータ、５０１…アクセス要求、５０２…認証要求、５０３…ユーザ認証要求、５０４…ユーザマスタ鍵、５０５…シーケンス番号、５０６…ユーザＩＤ、５０７，５１０…チャレンジコード、５０８…ユーザマスタ鍵、５０９…暗号化チャレンジコード、６０１…セッション鍵、６０２…送信側のユーザのマスター鍵、６０３…受信側のユーザのマスター鍵、６０４，６０５…暗号文、６０６…スクランブル鍵、６０７…デスクランブル鍵、６０８，６０９…暗号文、７０１…セッション鍵発行要求、７０２…発行されたセッション鍵、７０３…マスター鍵更新要求、８０１…否認防止要求、８０２，８０３…否認防止ファイル、１０１０…アクセス管理部、１０２０…ネットワーク通信管理部、１０３０…暗号化通信処理部、１０４０…鍵管理部、１０５０…否認防止管理部、１０６０…鍵回復部、１５０１…スクランブル鍵、１５０２，１５０３…デスクランブル鍵、１５０４，１５０５…データ、１５０６…暗号文、１５０７…公開鍵、１５０８…暗号化デスクランブル鍵、１５１０

…ユーザのマスター鍵としての秘密鍵、ｆ１１…通信管理セキュリティ機能、ｆ１２…ネットワーク送受信管理機能、ｆ１３…スクランブル機能、ｆ１４…デスクランブル機能、ｆ１５…通信構成管理機能、ｆ２１…ユーザセキュリティ機能、ｆ２２…データファイル処理機能、ｆ４１…鍵構成管理機能、ｆ４２…否認防止機能、ｆ４３…鍵回復機能。

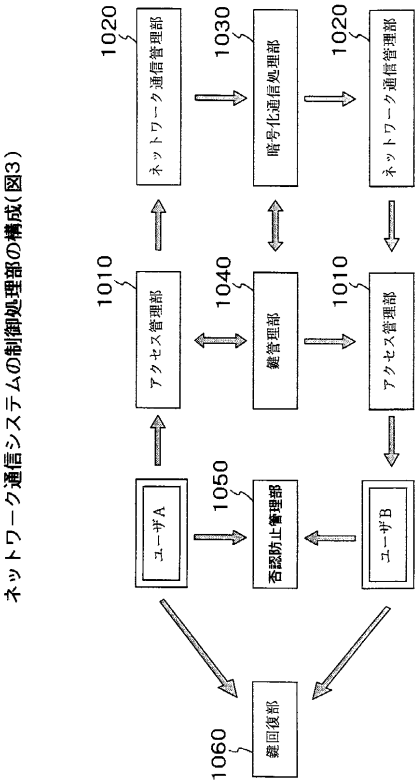
【図１】



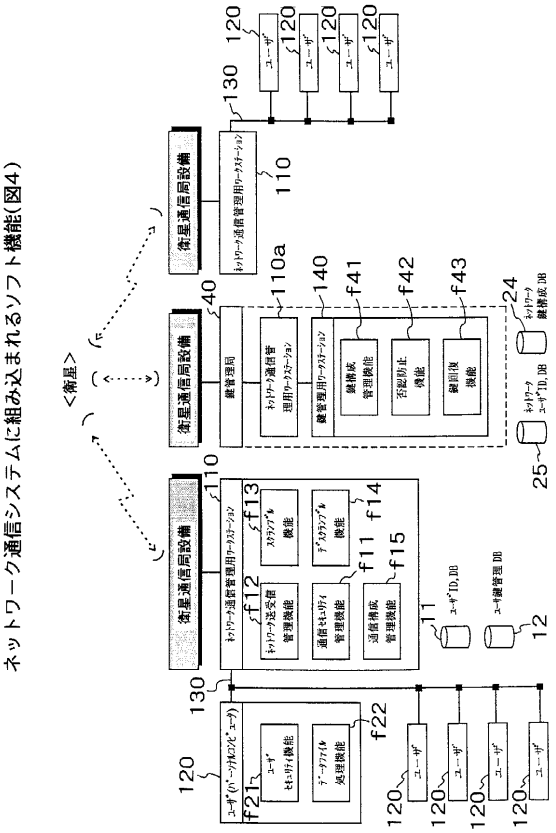
【図２】



【図３】

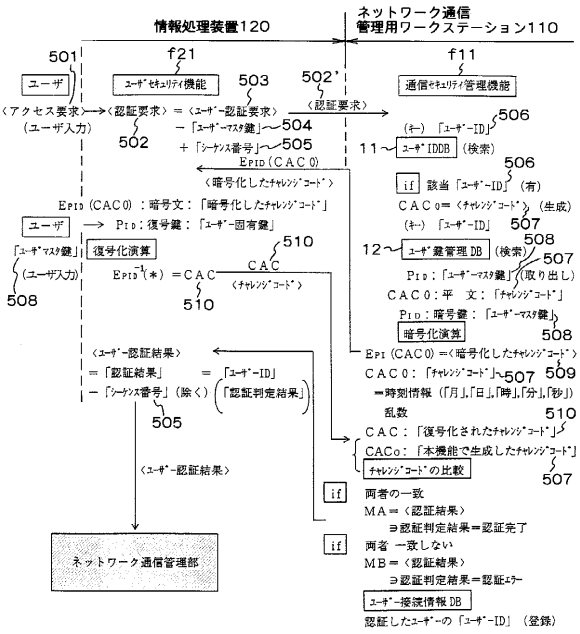


【図４】

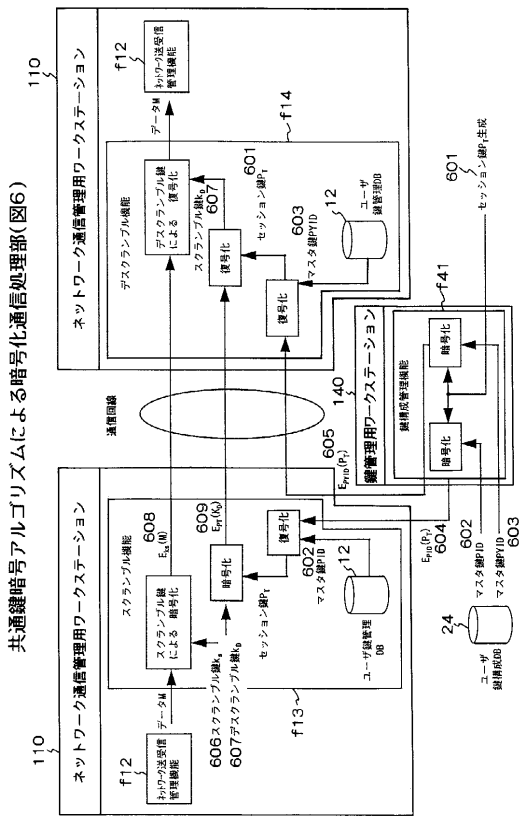


【図５】

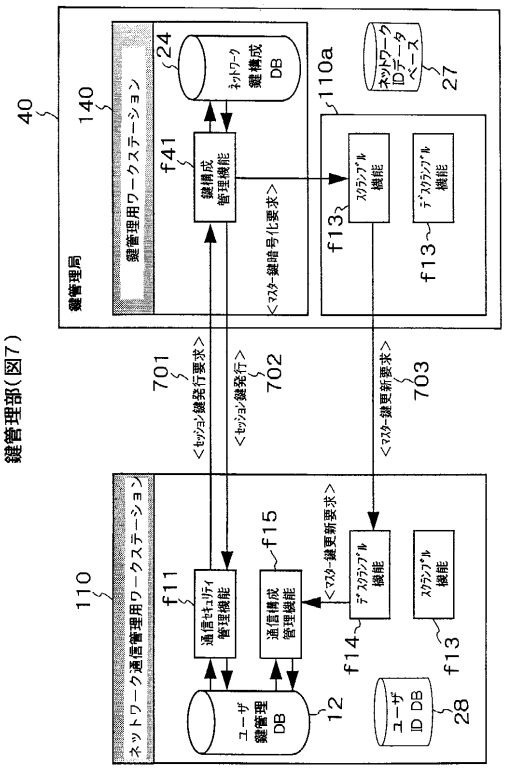
共通鍵暗号アルゴリズムによるアクセス管理部のソフト機能構成(図5)



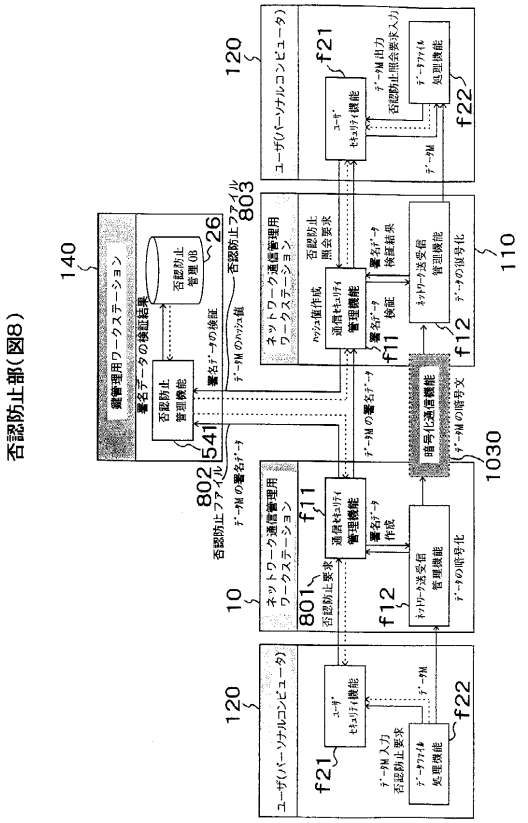
【図６】



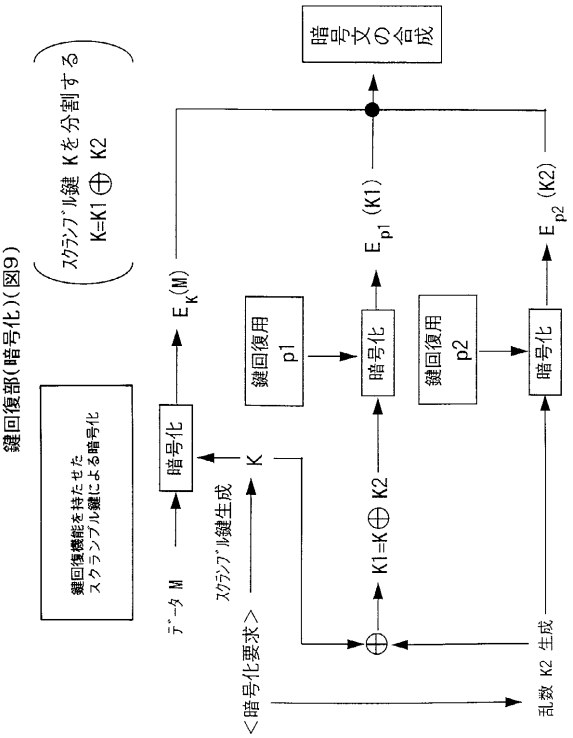
【図７】


鍵管理部(図7)
40
鍵管理局
140
鍵管理用ワークステーション
f41
鍵構成管理機能
24
ネットワーク鍵構成DB
110a
f13
スクランブル機能
デスクランブル機能
ネットワークIDデータベース
27
<マスター鍵暗号化要求>
701
<セッション鍵発行要求>
702
<セッション鍵発行>
703
<マスター鍵更新要求>
110
ネットワーク通信管理用ワークステーション
f11
通信セキュリティ管理機能
f15
通信構成管理機能
f14
デスクランブル機能
f13
スクランブル機能
ユーザ鍵管理DB
12
ユーザID DB
28

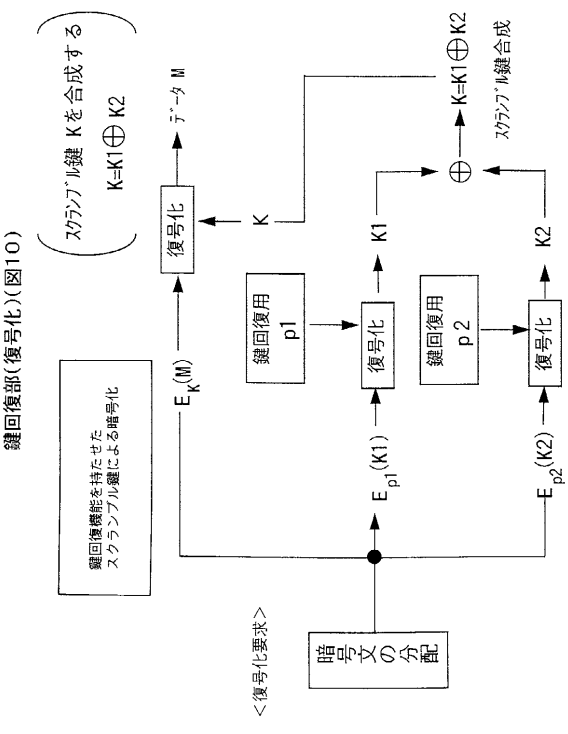
【図８】


否認防止部(図8)
140
鍵管理用ワークステーション
署名データの検証結果
否認防止管理機能
否認防止管理DB
26
541
802
否認防止ファイル
803
否認防止ファイル
120
ユーザ(パーソナルコンピュータ)
f21
ユーザセキュリティ機能
データM入力否認防止要求
データファイル処理機能
f22
10
ネットワーク通信管理用ワークステーション
801
否認防止要求
f11
通信セキュリティ管理機能
f12
ネットワーク送受信管理機能
暗号化通信機能
1030
110
ハッシュ値作成
署名データ作成
署名データ検証
データMの署名データ
データMのハッシュ値
データMの署名データ
データMの検証
データMの暗号文
データの暗号化
データの復号化
否認防止照会要求
署名データ検証結果
データM出力否認防止照会要求入力

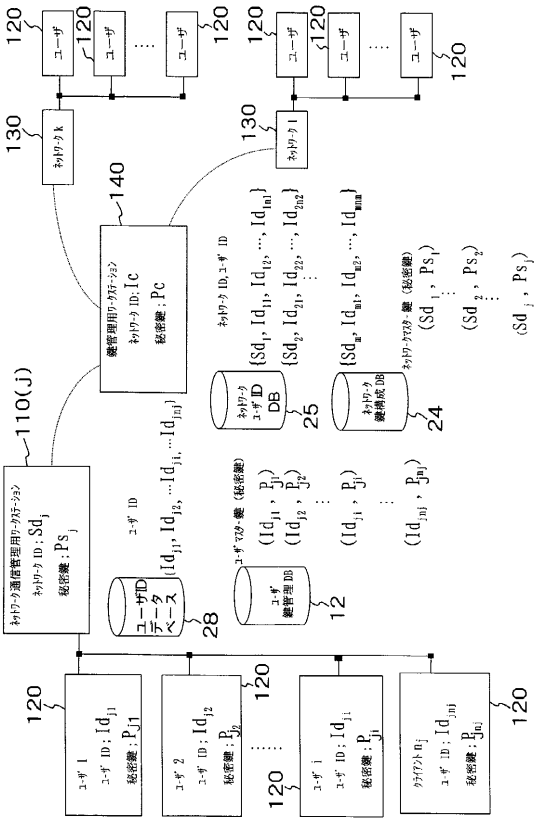
【図９】


鍵回復(暗号化)(図9)
鍵回復機能を持たせたスクランブル鍵による暗号化
(スクランブル鍵 Kを分割する K=K1⊕K2)
データ M
暗号化
$E_K(M)$
スクランブル鍵生成
K
鍵回復用 p1
鍵回復用 p2
暗号化
暗号化
$E_{p1}(K1)$
$E_{p2}(K2)$
暗号文の合成
K1=K⊕K2
<暗号化要求>
乱数 K2 生成

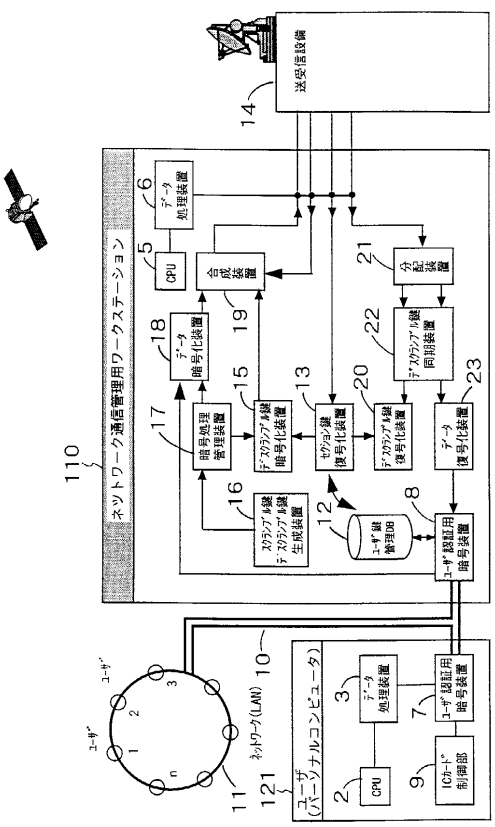
【図１０】


鍵回復(復号化)(図10)
鍵回復機能を持たせたスクランブル鍵による暗号化
(スクランブル鍵 Kを合成する K=K1⊕K2)
$E_K(M)$
復号化
データ M
K
鍵回復用 p1
鍵回復用 p2
$E_{p1}(K1)$
$E_{p2}(K2)$
復号化
復号化
K1
K2
K=K1⊕K2
スクランブル鍵合成
暗号文の分配
<復号化要求>

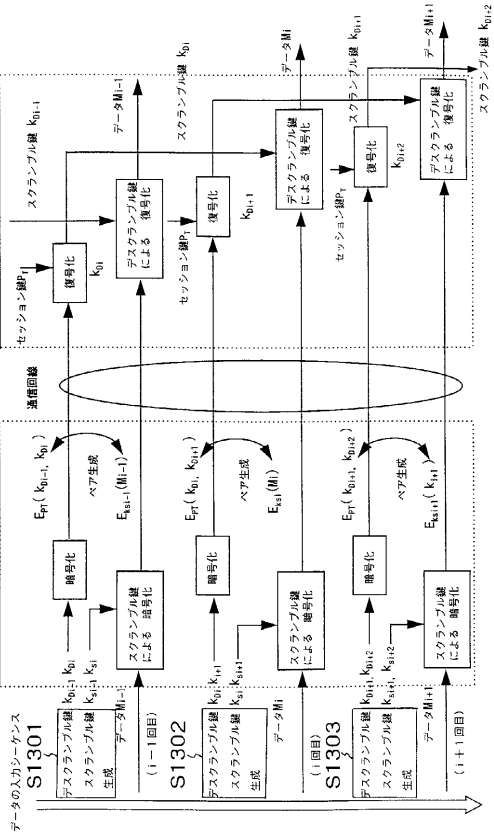
【図１１】



【図１２】

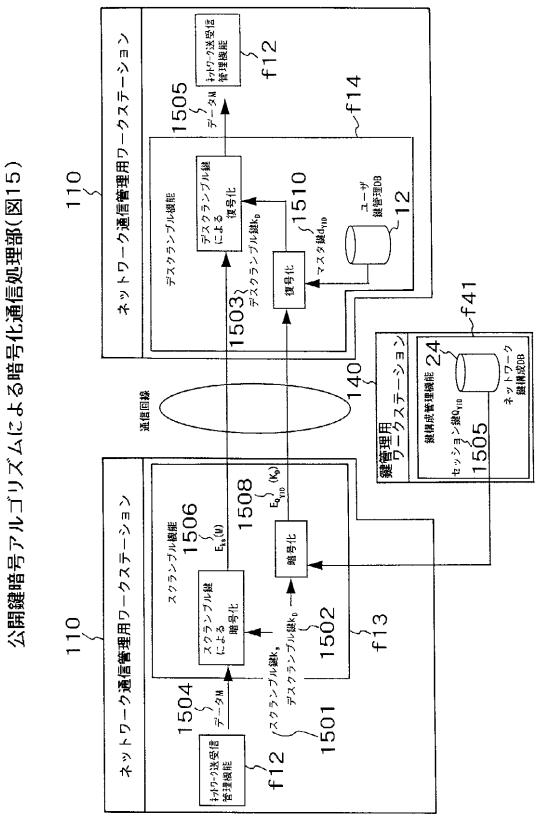


【図１３】

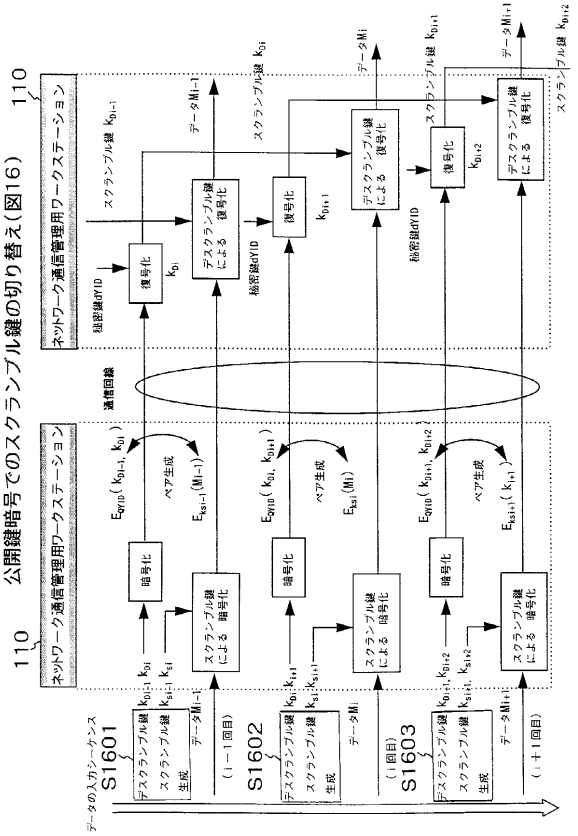


【図１４】

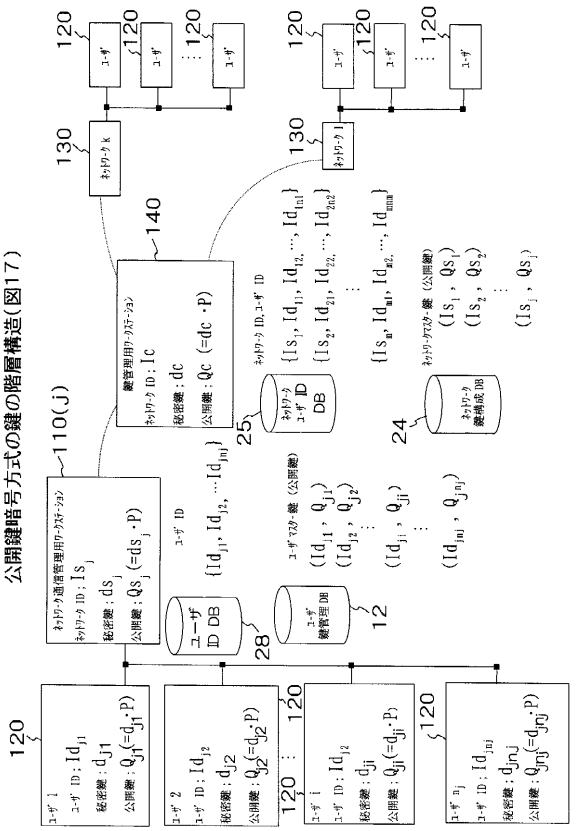
【図１５】


公開鍵暗号アルゴリズムによる暗号化通信処理部(図15)
ネットワーク通信管理用ワークステーション
110
通信回線
140
鍵管理用ワークステーション
スクランブル機能
デスクランブル機能
スクランブル鍵による暗号化
デスクランブル鍵による復号化
暗号化
復号化
ユーザ鍵管理DB
ネットワーク鍵構成DB
ネットワーク送受信管理機能
データM
スクランブル鍵
デスクランブル鍵
マスタ鍵
セッション鍵
1501
1502
1503
1504
1505
1506
1508
1510
f12
f13
f14
f41
12
24

【図１６】


公開鍵暗号でのスクランブル鍵の切り替え(図16)
ネットワーク通信管理用ワークステーション
110
通信回線
秘密鍵dYID
スクランブル鍵
暗号化
復号化
デスクランブル鍵による復号化
スクランブル鍵による暗号化
ペア生成
データの入力シーケンス
S1601
S1602
S1603
(i-1回目)
(i回目)
(i+1回目)

【図１７】


公開鍵暗号方式の鍵の階層構造(図17)
110(j)
ネットワーク通信管理用ワークステーション
鍵管理用ワークステーション
ユーザID DB
ユーザ鍵管理DB
ネットワークID DB
ネットワーク鍵構成DB
ユーザ
ネットワーク
120
130
140
12
24
25
28

フロントページの続き

(72)発明者　速水　洋志
神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立製作所　宇宙技術推進本部内
(72)発明者　谷口　英宣
神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立製作所　宇宙技術推進本部内
(72)発明者　白木　光彦
神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立製作所　宇宙技術推進本部内

合議体
審判長　吉岡　浩
審判官　石田　信行
審判官　鈴木　匡明

(56)参考文献　特開平５－３０４５２３（ＪＰ，Ａ）
特開平９－１９１３１８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L9/00