(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3618508号
(P3618508)
(45)発行日　平成17年2月9日(2005.2.9)　(24)登録日　平成16年11月19日(2004.11.19)

(51)Int.Cl.[7]　F I
H04L 12/18　H04L 12/18

請求項の数 8　(全 33 頁)

(21)出願番号　特願平9-53736
(22)出願日　平成9年3月10日(1997.3.10)
(65)公開番号　特開平10-32573
(43)公開日　平成10年2月3日(1998.2.3)
審査請求日　平成12年12月13日(2000.12.13)
(31)優先権主張番号　特願平8-61351
(32)優先日　平成8年3月18日(1996.3.18)
(33)優先権主張国　日本国(JP)

前置審査

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100083161
弁理士　外川　英明
(72)発明者　橋本　幹生
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝　研究開発センター内

審査官　▲高▼橋　真之

最終頁に続く

(54)【発明の名称】受信プロトコル装置及び同報メッセージ送信装置

(57)【特許請求の範囲】
【請求項１】
同一のメッセージを、１つ以上の送信装置から予め定められた複数の受信装置に送信する、これらの装置が接続された通信網を介した同報通信システムにおける受信プロトコル装置において、
送信装置から送信された同一のメッセージを同時に複数の上位実行装置に送信して処理を行うために、前記送信装置が送信したメッセージに含まれる時刻情報を送信時刻として設定する時刻設定手段と、
前記送信装置からのメッセージを前記複数の上位実行装置に送信するのに先だって、前記時刻設定手段によって設定された時刻になるまでこのメッセージを保持する保持手段と、
前記受信プロトコル装置に対して固有に振られた識別子が記憶された識別子記憶部と、
この識別子記憶部に記憶された識別子を第３者が取得することを禁止する第１の禁止手段と、
前記送信装置におけるメッセージの暗号化に用いられる暗号化鍵と同一の暗号化鍵を保持するための暗号鍵保持部と、
前記識別子記憶部に記憶された識別子を前記送信装置に送信して認証を受けることにより前記暗号化鍵を取得し、前記暗号鍵保持部に記憶する暗号化鍵取得手段と、
前記暗号化鍵取得手段による認証のときに、第３者による前記識別子の傍受を禁止する第２の禁止手段と、
前記送信装置から送信された暗号化メッセージをこの暗号化鍵保持部に保持された暗号化

鍵を用いて復号化する復号化手段と、
を具備し、この復号化されたメッセージを前記時刻設定手段によって設定された時刻になるまで前記保持手段に保持するようにしたことを特徴とする受信プロトコル装置。
【請求項２】
同一のメッセージを、１つ以上の送信装置から予め定められた複数の受信プロトコル装置に送信する、これらの装置が接続された通信網を介した同報通信システムにおける同報メッセージ送信装置において、
各受信プロトコル装置が予め定められた識別子を持つか否かを認証する認証手段と
この認証手段によって認証された受信プロトコル装置のみに所定の暗号化鍵を予め配布する配布手段と、
各受信プロトコル装置に配布した暗号化鍵と同一の暗号化鍵を用いて送信メッセージを暗号化して各受信プロトコル装置に送信する送信手段と、
予め定められた同報群の受信装置にメッセージを送信し、メッセージ送信後、予め定められたある時間Ｔｓ以内に確認応答を返さない受信装置がある場合には、該受信装置に対して予め定められたある回数Ｓｍａｘまで前記メッセージを１対１の送信によって再送することを試みる手段と、
　前記メッセージのメッセージリリース時刻を決定するメッセージリリース時刻決定手段と、
　予め定められた同報群の受信装置にリリース時刻通知を送信し、メッセージ送信後、予め定められたある時間Ｔｓ以内に確認応答を返さない受信装置がある場合には、該受信装置に対して予め定められたある回数Ｗｍａｘまで前記リリース時刻通知を１対１の通信によって再送することを試みる手段を備えたことを特徴とする同報メッセージ送信装置。
【請求項３】
送信装置から同報された同報メッセージを受信し、該メッセージに対する確認応答を１対１の通信によって前記送信装置に送信する第１の確認応答手段と、
送信装置から同報されたリリース時刻通知を受信し、該リリース時刻通知の確認応答を返す第２の確認応答手段と、
当該メッセージに含まれるリリース時刻を、対応する受信済みメッセージ毎に記憶する手段と、
前記メッセージ毎に記憶したリリース時刻に、対応するメッセージを上位実行装置に送信する手段とを
備えたことを特徴とする請求項１に記載の受信プロトコル装置。
【請求項４】
送信装置から同報された同報メッセージを受信し、該メッセージに対する確認応答を１対１の通信によって前記送信装置に送信する手段と、
送信装置から同報されたリリース時刻通知を受信し、当該メッセージに含まれるリリース時刻を対応する受信済みメッセージ毎に記憶する手段と、
前記メッセージ毎に記憶したリリース時刻に、対応するメッセージを上位実行装置に送信する手段と、
該送信に成功した場合に送信装置にリリース成功メッセージを送信する手段とを
備えたことを特徴とする請求項１に記載の受信プロトコル装置。
【請求項５】
送信装置から同報された同報メッセージを受信し、該メッセージに対する確認応答を１対１の通信によって前記送信装置に送信する手段と、
送信装置から同報されたリリース時刻通知を受信し、当該メッセージに含まれるリリース時刻を対応する受信済みメッセージ毎に記憶する手段と、
前記メッセージ毎に記憶したリリース時刻に、対応するメッセージを上位実行装置に送信する手段とを
備えたことを特徴とする請求項１に記載の受信プロトコル装置。
【請求項６】

送信装置から同報された同報メッセージを受信し、該メッセージに対する確認応答を１対１の通信によって前記送信装置に送信する手段と、
送信装置から同報されたメッセージ及びリリース時刻通知を受信し、確認応答を返す手段と、
当該メッセージに含まれるリリース時刻を対応するメッセージ毎に記憶する手段と
前記メッセージ毎に記憶したリリース時刻に、対応するメッセージを上位実行装置に送信する手段とを
備えたことを特徴とする請求項１に記載の受信プロトコル装置。
【請求項７】
送信装置から同報された同報メッセージを受信し、該メッセージに対する確認応答を１対１の通信によって前記送信装置に送信する手段と、
送信装置から同報されたメッセージ及びリリース時刻通知を受信し、確認応答を返す手段と、
当該メッセージに含まれるリリース時刻を対応するメッセージ毎に記憶する手段と、
前記メッセージ毎に記憶したリリース時刻に、対応するメッセージを上位実行装置に送信する手段と、
該送信に成功した場合に送信装置にリリース成功メッセージを送信する手段とを
備えたことを特徴とする請求項１に記載の受信プロトコル装置。
【請求項８】
送信装置から同報された同報メッセージとメッセージ本体及びリリース時刻通知を受信する手段と、
当該メッセージに含まれるリリース時刻を対応する受信済みメッセージ毎に記憶する手段と、
前記メッセージ毎に記憶したリリース時刻に、対応するメッセージを上位実行装置に送信する手段とを
備えたことを特徴とする請求項１に記載の受信プロトコル装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は送受信プロトコル装置に関し、特に、通信網を介して１つのメッセージを複数の装置に同報通信する場合において、送受信プロトコル装置の間でメッセージの配送時間の公平性、公正性を確保する装置に関する。
【０００２】
【従来の技術】
同報通信は通信網を用いた放送や、分散情報処理のアプリケーションに有用な通信方式である。
コンピュータアプリケーションや情報提供サービスにおいては信頼性の高い同報通信方式が求められる。また、同報通信の特質をより生かすために、全ての受信装置において同じ結果が得られるという性質も求められる場合がある。この性質は、例えばデータを分散して格納する際にデータの同一性を保つ方式や、加入者間で公平な情報提供サービスの方式に応用が可能である。
【０００３】
これらの要求に対して次の様な性質を保証するプロトコルが提案、実現されている。ここでは同一の同報メッセージを受信する受信装置の集合を同報群と呼ぶ。
【０００４】
（原子性）
あるメッセージの配送について全ての受信装置で受信されない限りそのメッセージは配送されない。すなわち、ある受信装置で同報メッセージが受信されれば同じ同報群に属する他の全ての受信装置にそのメッセージが配送されていることが保証される。
【０００５】

（順序同値）
同報群の全ての受信装置でメッセージの受信情報が同一になること。同報通信の信頼性を低くする原因の中で大きなものはメッセージ伝送のビット誤りや伝送中の廃棄である。ビット誤りは伝送路の誤りによって生じ、廃棄は輻輳（ここでの輻輳はパケット網やＡＴＭ網における輻輳を指す）によって生じる。ビット誤りについては端末間で誤り訂正技術を摘要することにより、廃棄については再送を行うことによりメッセージ配送失敗の確率を低くすることができる。もちろん再送はビット誤りに起因するメッセージ配送失敗にも効果があるが、メッセージが完全に失われるほどの時間にわたる輻輳には誤り訂正技術は有効ではない。輻輳に対して信頼性を確保するには再送の技術が不可欠である。

【０００６】
一方、全ての受信装置で同一の受信結果が得られるという性質を実現するにはメッセージ配送の失敗及び伝送遅延の不均一性が障害となる。メッセージ配送の失敗は上記のように再送によって回復できるが、再送を行うことによってメッセージの配送時刻が送れてしまう。また、伝送遅延の差はメッセージの配送時間に影響する。

【０００７】
以下に、上記した２つの性質を満たす同報通信を実現した従来の技術について説明する。同報群のメッセージの送受信を管理する装置をマスタとよぶ。メッセージを受信する装置をクライアントと呼ぶ。メッセージを送信する装置をセンダと呼ぶ。マスタ、クライアント、センダはそれぞれ同報通信のプロトコルを処理する機能部分と、そのプロトコル処理の機能を利用して同報通信のアプリケーションを行う機能部分とに概念的に分けられる。

【０００８】
ここで、同報による株価情報の提供を例としよう、アプリケーションは、センダでは株価情報の放送を行う部分であり、受信側はその情報を処理する部分、例えばその情報に基づいて電子化した取り引きを行う部分にある。

【０００９】
プロトコル処理機能とアプリケーション機能は概念的には分けられるが、一般にその実装は明確に分離されていない。多くのパーソナルコンピュータの場合、ソフトウェアの機能部分としてはプロトコル処理機能とアプリケーション機能が分けられていたとしても、どちらの機能も同一のメモリ空間の上で、同一のプロセッサによって実行される。

【００１０】
以下に図１５に従って同報受信の手順を説明する。
マスタ７０１は同報コネクションを通じてクライアントＡ７０２，Ｂ７０３にメッセージを送信する。メッセージには連続した順序関係を持つ識別子が与えられる。識別子ｐのメッセージをM_p　と表記する。

【００１１】
クライアントＡ７０２，Ｂ７０３はM_p　を受信するとそれぞれ確認応答ACK_p　（Ａ），ACK_p　（Ｂ）をマスタ７０１に送信する。確認応答にはメッセージ識別子ｐとクライアント識別子が含まれる。この応答は同報する必要はない。マスタ７０１は全てのクライアント、ここではクライアントＡ７０２，Ｂ７０３からの確認応答ACK_p　（Ｘ）を確認するとメッセージリリース許可REL_p　（ｉ）を同報する。ｉはリリース許可の出たメッセージの識別子で、リリース許可の出た順番にｉ，ｉ＋１，…のように付けられる。

【００１２】
次に、図１６に従って同報受信のメッセージ消失があった場合の手順を説明する。ここで表記などは図１５と同じである。
マスタ７０１は同報コネクションを通じてクライアントＡ７０２，Ｂ７０３にメッセージM_p　を送信する。マスタ７０１は送信と同時にタイマＴ１をセットする。クライアントＡ７０２は時刻t_0　にM_p　を受信する。一方、クライアントＢ７０３へのメッセージは消失したとする。このときサーバはタイマＴ１のタイムアウト時点でメッセージＭｐに対応するクライアントＢ７０３からの確認応答が到着していないことを検出し、メッセ

ージのM_p　の再送を行う。クライアントＢ７０３はM_p　を受信すると確認応答ACK_p　（Ｂ）を送信する。マスタ７０１はACK_p　（Ｂ）を受信すると全てのクライアントの確認応答がそろうので、メッセージリリース許可REL_p　（ｉ）を同報する。

【００１３】

メッセージの再送では全てのクライアントにメッセージが同報され、それを受信したクライアントは既に確認応答したメッセージに対しても再度確認応答を送信する。これによって確認応答ACK_p　（Ｘ）が消失した場合でも、タイムアウト後の再送に対する確認応答でマスタ７０１は全てのクライアントがメッセージを受信したことを知ることができる。

【００１４】

以下に、図１７に従って同報受信のリリース許可メッセージの消失があった場合の手順を説明する。表記などは図１５と同じである。

ここでメッセージM_p　に対するクライアントＢ７０３へのリリース許可メッセージREL_p　（ｉ）が消失した場合を示している。クライアントＡはリリース許可メッセージを正常に受信し、時刻t_2　にメッセージM_p　をリリースしている。

【００１５】

クライアントＢ７０３ではメッセージＭｐ　がリリースされないまま次のメッセージM_{p+1}　の受信手続きが正常に行われ、そのリリース許可メッセージREL_{p+1}　をクライアントＢ７０３が受信する。クライアントＢ７０３はリリース許可メッセージの識別子ｐ＋１を直前に受信したリリース許可メッセージの識別子ｐ－１と比較し、不連続を検出する。クライアントＢ７０３は不連続を検出するとリリース許可メッセージの消失と判断し、対応するメッセージをリリースする。この場合は識別子ｐ－１とｐ＋１の間のｐに対応するメッセージM_p　をリリースする。

【００１６】

メッセージはリリース許可メッセージの識別子の不連続を検出してリリースされるので、メッセージM_p　はメッセージM_{p+1}　の前にリリースされて受信順序は保たれる。

【００１７】

以下に、図１８に従ってメッセージ配送失敗の場合の手順を説明する。表記などは図１５と同じである。マスタ７０１は同報コネクションを通じてクライアントＡ７０２，Ｂ７０３にメッセージM_p　を送信する。マスタ７０１は送信ど同時にタイマＴ１をセットする。

【００１８】

クライアントＡ７０２は時刻t_0　にM_p　を受信する。一方クライアントＢ７０３へのメッセージは消失する。サーバはタイマＴ１のタイムアウト時点でメッセージM_p　に対応するクライアントＢ７０３からの確認応答が到着していないことを検出し、メッセージM_p　の再送を行う。この手順を予め定められた回数ｎ回繰り返してもクライアントＢ７０３から受信確認応答が得られない場合にはそのメッセージ配送は失敗として、マスタ７０１は送信失敗メッセージ$FAIL_p$　を同報する。送信失敗メッセージを受信したクライアンとＡ７０２はメッセージM_p　の配送を取りやめる。

【００１９】

上記のプロトコルには次の２つの問題がある。

１．伝送遅延による不公平

図１６においてクライアントＡ７０２がリリース許可を受信する時刻t_3　とクライアントＡ７０２がリリース許可を受信する時刻t_2　には、伝送遅延の差によるt_d　の時間差がある。この差がアプリケーションにメッセージが渡される時刻と不公平となる。

２．メッセージの早取り

クライアントＡ７０２は、メッセージM_p　を受信してすぐの時点t_0　でメッセージを読んでしまうことができる。もちろんプロトコル規約上はこのようなことは許されていないが、このような違反が行われているかどうかを他のネットワーク装置から検査することは、プロトコルの実装を検査しない限り無理である。

【００２０】
また、クライアント装置のプロトコル実装は正当なものであったとしても、ネットワーク上の装置、または当該クライアント装置内の機能がメッセージを傍受していれば、メッセージを他のクライアント装置よりも早く読むことが可能である。上述のパーソナルコンピュータの場合では、アプリケーション機能がプロトコル処理の作業メモリを読むことで傍受が可能であり、受信装置がユーザ側の装置としてあれば、このような変更を加えることは容易である。
【００２１】
（複数の送信者がいる場合）
次に複数の送信者がいる同報網において、全てのクライアントのメッセージ受信順序を一致させる従来の技術について説明する。
【００２２】
図１９に従って説明する。ここで、同報群はマスタ８０１、クライアントＡ８０２，Ｂ８０３，センダａ８０４，ｂ８０５からなる。
センダａ８０４は時刻t_0にメッセージM_p^aを同報する。M_p^aはセンダａ８０４から送られた識別子ｐを持つメッセージであることを表す。ｐはセンダａについて一意の識別子であるクライアントＡ８０２，Ｂ８０３はメッセージM_p^aを受信するとそれぞれACK_p^a（Ａ），ACK_p^a（Ｂ）をセンダａ８０４に送信する。
センダａ８０４は全てのクライアントからＡＣＫを受信すると、メッセージリリース許可要求$RELREQ_p^a$をマスタ８０１に送信する。
【００２３】
メッセージリリース許可要求$RELREQ_p^a$（ｉ）を受信したマスタ８０１はメッセージリリース許可要求$RELREQ_p^a$（ｉ）を同報する。リリース許可を受信したクライアントはメッセージをリリースする。
【００２４】
次に複数の送信者のメッセージ送信の手順を説明する。
センダａ８０４は時刻t_1にメッセージM_{p+1}^aを同報する。その後、センダｂ８０５は時刻ｔ２にメッセージM_q^bを同報する。これらのメッセージを受信したクライアントＡ８０２，Ｂ８０３はそれぞれ確認応答ACK_{p+1}^a（Ａ），ACK_q^b（Ａ），ACK_{p+1}^a（Ｂ），ACK_q^b（Ｂ）をセンダａ８０４，ｂ８０５に送り、各センダはＡＣＫに揃った時点でリリース要求$RELREQ_{p+1}^a$，$RELREQ_q^b$をマスタ８０１に送信する。
【００２５】
クライフントＡ８０２，Ｂ８０３におけるメッセージの受信順序は、伝送遅延、遅延揺らぎなどによって必ずしも送信の順序と一致しない。
マスタ８０１はリリース要求を受けとったメッセージからリリース許可を同報する。リリース許可には同報群について一意の識別子ｉ，ｉ＋１，…が付与されている。そのため、クライアントＡ８０２，Ｂ８０３でリリース許可の受信に失敗したり、受信順序が逆転してもこれらのクライアントはそれを検出することができ、全てのクライアントでサーバが判断したメッセージのリリース順序が保たれる。
【００２６】
ここでクライアントＡ８０２ではセンダｂ８０５からのメッセージが先に到着したが、クライアントＢ８０３ではセンダａ８０４からのメッセージが先に到着している。センダａ８０４は全てのクライアントの確認応答が揃うのを待つことになり、リリース要求の送信はセンダｂ８０５よりも遅くなる。
【００２７】
マスタ８０１はリリース要求の受け付け順序に従ってリリース許可を出すため、マスタ８０１へのリリース要求の到着がもっとも遅いメッセージが、リリースがもっとも遅くなる。
【００２８】

ここで、センダａ８０４が時刻t_1に送信したメッセージはマスタ８０１とクライアントＢ８０３ではセンダｂ８０５が遅れて時刻t_2に送信したメッセージより早く到着している。しかし、クライアントＡ８０２ではセンダｂ８０５のメッセージがセンダａ８０４よりも早く到着している。結局、先に送信されていても、マスタ８０１にＡＣＫが到着するのが遅いセンダａ８０４のメッセージのリリースが後から送信されたセンダｂ８０５のメッセージのリリースよりも遅れてしまう。

【００２９】

更に、プロトコルの実装に不正があった場合、故意にメッセージの確認応答をを返さないことにより、そのメッセージのリリース時刻を遅延させることができる。センダとクライアントが一体であった場合、他のセンダからのメッセージを受信した後にメッセージを送信し、その後に受信メッセージに対するＡＣＫを送信することによって、他のクライアントに対してあたかも自装置が先にそのメッセージを送信したかのように受信順序を変えてしまうことができる。

【００３０】

このように複数のセンダのある同報プロトコルでは、全てのクライアントで受信メッセージの順序関係が保たれるものの、必ずしも異なるセンダの間で送信側のメッセージ送出の時間関係が保存されるわけではない。

【００３１】

特に、伝送遅延に揺らぎのある通信網を利用した場合、これらの影響を補正することは困難である。また、再送が発生した場合、あたかもメッセージの到着が遅れたことと同じ効果が出てしまう。

【００３２】

複数のセンダのある同報プロトコルには、伝送遅延の差や再送による確率的に発生するメッセージ配送の遅れを原因賭する不公平性が存在するが、メッセージの識別番号に基づいたプロトコルの上でこの問題を解決することは原理的に不可能である。この問題の１つの解決方法として、センダでメッセージの送信時刻を付与し、受信側でその時刻を評価してメッセージ受信順序を決定する方法が知られている（Ｂｉｒｍａｎ，Ｋ．，Ｓｃｈｉｐｅｒ，Ａ．，Ｓｔｅｐｈｅｎｓｏｎ，Ｐ．：”Ｌｉｇｈｔｗｅｉｇｈｔ Ｃａｕｓａｌ ａｎｄ Ａｔｏｍｉｃ Ｇｒｏｕｐ Ｍｕｌｔｉｃａｓｔ”，ＡＣＭ Ｔｒａｎｓ．Ｃｏｍｐｕｔｅｒ ｓｙｓｔｅｍｓ，９（３）：２７２－，１９９１）ところが、この方法ではセンダが時刻を偽ることによってメッセージ順序を操作するのを防ぐことはできない。

【００３３】

以上に説明したように、原子性、順序同値性をプロトコルによって保証したとしても、アプリケーションがメッセージを読むまでの時間について見た場合、及び不正なプロトコル処理が行われる可能性を考慮すれば必ずしも公平とはいえなかった。これは、電子商取引や、取り引きに影響を与えるニュースの配送に同報通信を用いる上で障害となる。

【００３４】

【発明が解決しようとする課題】

すなわち、従来技術には、第１に、メッセージリリース時間の不公平の問題がある。すなわち、伝送遅延の差によってメッセージが利用可能になる時刻に不公平が生じてしまう。第２に、プロトコル実装違反の可能性がある。すなわち、メッセージの受信失敗を偽ることによって他の受信端末の受信を送らせることができてしまう。更に、受信メッセージを読んでから自装置が送信したメッセージを他のクライアントには逆のメッセージ順序と判断させることができる。第３に、メッセージの傍受の問題がある。すなわち、他の受信者がメッセージを受信できていない状態（受信確認状態）でアプリケーションがメッセージを読んでしまう可能性がある。

【００３５】

本発明はこのような課題に着目してなされたものであり、その目的とするところは、伝送遅延の差や再送による確率的なメッセージ配送の遅れによらず、同報メッセージ受信時刻

の受信時刻を一致させるとともに、ユーザから見たメッセージ送信時間すなわちアプリケーションが同報プロトコル装置にメッセージを渡した時刻が、他の受信装置において正しく受信順序に反映されるようにして、送受信装置の間でメッセージの配送時間の公平性、公正性を保証することができる受信プロトコル装置、同報メッセージ送信装置、及び送受信プロトコル装置を提供することにある。

【００３６】

【課題を解決するための手段】

上記の目的を達成するために、第１の発明は、同一のメッセージを、１つ以上の送信装置から予め定められた複数の受信装置に送信する同報通信システムにおける受信プロトコル装置において、送信装置から送信された同一のメッセージを同時に複数の上位実行装置に送信して処理を行うために、送信時刻を他の受信プロトコル装置との間で予め合意した時刻に設定する時刻設定手段と、前記送信装置からのメッセージを前記複数の上位実行装置に送信するに先だって、前記時刻設定手段によって設定された時刻になるまでこのメッセージを保持する保守手段とを具備する。

【００３７】

また、第２の発明は、当該受信プロトコル装置を他の受信プロトコル装置から識別するための識別子が記憶された識別子記憶部と、この識別子記憶部に記憶された識別子への第３者からのアクセスを禁止する第１の禁止手段と、前記識別子記憶部に記憶された識別子を前記送信装置に送信して認証を行うときに、第３者による前記識別子の傍受を禁止する第２の禁止手段と、前記送信装置におけるメッセージの暗号化に用いられる暗号化鍵と同一の暗号化鍵を保持するための暗号化鍵保持部と、前記送信装置から送信された暗号化メッセージをこの暗号化鍵保持部に保持された暗号化鍵を用いて復号化する復号化手段とを具備し、この復号化されたメッセージを前記時刻設定手段によって設定された時刻になるまで前記保持手段に保持する。

【００３８】

また、第３の発明は、同一のメッセージを、１つ以上の送信装置から予め定められた複数の受信プロトコル装置に送信する同報通信システムにおける同報メッセージ送信装置において、各受信プロトコル装置が予め定められた識別子を持つか否かを認証する認証手段と、この認証手段によって認証された受信プロトコル装置のみに所定の暗号化鍵を予め配布する配布手段と、各受信プロトコル装置に配布した暗号化鍵と同一の暗号化鍵を用いて送信メッセージを暗号化して各受信プロトコル装置に送信する送信手段とを具備する。

【００３９】

また、第４の発明は、前記認証手段が各受信プロトコル装置を識別するための識別子が記憶された識別子記憶部と、各受信プロトコル装置と通信を行うことにより、各受信プロトコル装置の識別子が前記識別子記憶部に含まれているか否かを確認する確認手段と、前記識別子が前記識別子記憶部に含まれている場合はその受信プロトコル装置を正規の受信プロトコル装置であると認定し、前記識別子が前記識別子記憶部に含まれていない場合はその受信プロトコル装置を正規の受信プロトコル装置ではないと認定する認定手段とを具備する

また、第５の発明は、前記認証手段が、前記同報メッセージ通信装置の外部に設けられた識別子記憶部に記憶された受信プロトコル装置識別のための識別子を用いて認証を行う。

【００４０】

また、第６の発明は、第１または第２の発明に係る受信プロトコル装置と、第３，４，または５の発明に係る同報メッセージ送信装置とから構成された送受信プロトコル装置。

【００４１】

また、第７の発明は、第２の発明に係る受信プロトコル装置と、第４の発明に係る同報メッセージ送信装置とを単一の装置によって構成した送受信プロトコル装置である。

【００４２】

更に、本発明は以下の特徴を有する。

すなわち、前記送信装置から送信されたメッセージが一意の送信時刻または送信順に関す

る情報を含み、前記受信プロトコル装置は、この送信時刻または送信順に関する情報に従って受信したメッセージを前記上位実行装置に送信する。

【００４３】

また、前記メッセージが複数の送信装置から送信されるメッセージであり、このメッセージが一意の送信時刻または送信順に関する情報を含む。

また、前記暗号化鍵を所定のタイミングで変更する。

【００４４】

また、前期メッセージが複数の送信装置から送信されるメッセージであり、前記受信プロトコル装置は、前記上位実行装置に前記メッセージを送信するときに、各送信装置に応じて送信タイミングを遅延させる。

また、前記受信プロトコル装置は、下位通信網の故障を検出したときに、この故障を記録する記憶手段を有する。

【００４５】

【発明の実施の形態】

まず、本発明の実施形態の概略を説明する。メッセージリリース時刻の問題を解決するにはクライアントの絶対時刻を合わせ、クライアントへのメッセージ転送時刻を一致させれば、ネットワークを通じた端末の時刻同期誤差の範囲で公平なメッセージ転送が可能になる。しかし、プロトコル実装違反の問題は決して同報プロトコル自体によっては解決しない。例えば送信メッセージに過去のタイムスタンプを付加することは、メッセージの紛失の可能性が有る限り防止できない。

【００４６】

また、仮にプロトコル処理に全く不正がなかったとしてもメッセージを格納するメモリを直接読み込むことにより、プロトコル上は受信状態になっていないメッセージを早取りすることは可能でありメッセージ傍受の問題は残る。この問題は、正規のプロトコル処理を行わない限りメッセージを手に入れることができなくするような暗号化を行うと同時に、復号化装置の内部情報の不正な読み出しを防止することによって解決することができる。

【００４７】

そこで、本実施形態では、第１に、プロトコル装置に同報群で同期した時計を設け、同報群でメッセージをアプリケーションに渡す時刻についての合意を行うこと、第２に、プロトコル装置を信頼できる機関によって認証されたものであるか否かを判定する手段をプロトコル及びその実装である装置に組み込むこと、第３に、同報メッセージを暗号化し、プロトコル装置はメッセージの復号化結果を蓄積し、同意した時刻に始めてメッセージを出力することによって上記課題を解決し、目標とする公平なプロトコル処理を可能にするものである。

【００４８】

以下に、図面を参照して本発明の一実施形態を詳細に説明する。図１は第１実施形態の基本構成を示す図である。図１において、１は同報送信装置，２は受信装置識別子テーブル，１１－１～ｎは同報受信クライアント装置（クライアント装置）を表し、１３－１～ｎは網側インタフェース装置（網インタフェース装置），１２－１～ｎは同報受信プロトコル装置（受信プロトコル装置），１１－１～ｎは同報受信クライアント装置（クライアント装置），１４－１～ｎは上位インタフェース点，１５－１～ｎは下位インタフェース点，１６－１は網側インタフェース点，１７－１～ｎは受信プロトコル装置識別子（受信装置識別子），３１は通信網をそれぞれ表す。３２－１はクライアント装置１１－１と同報送信装置１との間に設定されるポイントーポイントのコネクション，３３は同報送信装置１とクライアント装置１１－１から１１－ｎで構成される同報コネクションである。

【００４９】

網インタフェース装置１３－１～ｎと同報送信装置１及びそれらが接続される通信網３１は、網インタフェース装置１３－１～ｎ及び同報送信装置１の識別子が既知であればコネクション設定が可能であり、かつ同報機能を備えたものであれば、何であっても良い。ここでは各網インタフェース装置１３－１～ｎ及び同報送信装置１にはそれぞれ一意に識別

されるＥ．１６４形式のアドレスが付与され、ポイントーマルチポイントのコネクション設定手段を持つＡＴＭインタフェース仕様（ＡＴＭ　ｆｏｒｕｍ　ＵＮＩ　３．１　仕様，Ｔｈｅ　ＡＴＭ　Ｆｏｒｕｍ，１９９４）　を用いるものとする。ここではメッセージの同報を受信する装置の集まりを総称して同報群と呼ぶ

図２は、受信プロトコル装置１２－１～ｎの動作の概略を示すフローチャートである。Ｓ１０１は同報群加入手続き、Ｓ１１１は同報メッセージ受信手続き、Ｓ１２１は同報終了判断手続き、と１４１は受信エラー処理手続き、Ｓ１５１は同報群受信終了手続き、Ｓ１３１は鍵変更処理をそれぞれ表す。

【００５０】

図３は、受信プロトコル装置１２－１～ｎの同報群加入手続きＳ１０１の詳細を示すフローチャートである。Ｓ１０２はコネクション設定手続き、Ｓ１０３は受信プロトコル装置識別子の証明手続き、Ｓ１０４は同報送信装置１との暗号化鍵共有手続き、Ｓ１０５は同報復号化鍵取得手続きである。

【００５１】

図４は受信プロトコル装置１２－１～ｎの同報メッセージ受信手続きＳ１１１の詳細を示すフローチャートである。Ｓ１２２はメッセージ受信ステップ、Ｓ１２３は確認応答送信ステップ、Ｓ１２４はリリース許可受信タイムアウト判定ステップ、Ｓ１２５はリリース許可受信ステップ、Ｓ１２６はリリース許可確認応答送信ステップ、Ｓ１２７はメッセージ出力時刻判定ステップ、Ｓ１２８はリリース時刻再受信ステップ、Ｓ１３０は制御変数ｊ増分ステップ、Ｓ１３１は制御変数判定ステップ、Ｓ１３２はエラー処理、Ｓ１４０はメッセージ出力ステップである。

【００５２】

図５に同報メセージ受信手続きの正常時のメッセージシーケンスを示す。６０１は送信装置、６０２，６０３は受信装置Ａ，Ｂをそれぞれ表す。

図６に同報メセージ受信手続きのメッセージリリース許可の転送失敗時のメッセージシーケンスを示す。６０１は送信装置、６０２，６０３は受信装置Ａ，Ｂをそれぞれ表す。

【００５３】

図７に複数の送信者のメッセージ順序の合意を得る同報メッセージシーケンスをしめす。６１１はマスタ、６１２，６１３はクライアントＡ，Ｂ、６１４，６１５はセンダａ，ｂをそれぞれ表す。

【００５４】

図８に図１に示す同報送信装置１の機能ブロック図を示す。１は同報送信装置，２は受信プロトコル装置識別子テーブル、３は同報メッセージ入力端末、２０２は同報メッセージ入力機能、２０３は同報プロトコル状態管理機能、２０４は同報メッセージ暗号化機能、２０５はメッセージ認証子付加機能、２０６はメッセージ認証機能、２１１は時計機能、２１２は同報群管理機能、２１３はコネクション設定機能、２１４は装置識別子機能、２２１はネットワークインタフェース機能である。

図９に図１に示す受信プロトコル装置１２－１～ｎの機能ブロック図を示す。１４は上位インタフェース点、１５は下位インタフェース点、１７は受信プロトコル装置識別子、３０１は時計機能、３０２は上位インタフェース機能、３０３はメッセージ蓄積機能、３０４はメッセージ復号化機能、３０５は同報プロトコル状態管理機能、３０６はメッセージ認証子付加機能、３０７はメッセージ認証子検査機能、３０８は下記装置インタフェース機能、３０９はコネクション設定機能、３１０は受信メッセージ処理スケジューリング機能、をそれぞれ表す。

【００５５】

図１０に同報送信装置１の同報群管理動作の概略フローチャートを示す。Ｓ４０１は同報群初期化手続き、Ｓ４１１は同報群加入脱退要求手続き、Ｓ４２１は同報群加入受け付け手続き、Ｓ４３１は同報群脱退手続き、Ｓ４４１は同報群暗号化鍵変更手続き、Ｓ４５１は同報群通信終了判断手続きをそれぞれ表す。

【００５６】

図１１は同報送信装置１の同報群加入要求受け付け動作Ｓ４２１の詳細なフローチャートを示す。Ｓ４２２は受信装置認証手続き、Ｓ４２３は受信装置との通信鍵共有手続き、Ｓ４２４は同報の復号鍵配布手続き、Ｓ４２５は同報群設定手続き、Ｓ４２６は同報コネクション設定手続きをそれぞれ表す。

【００５７】

図１２に同報送信装置１の同報送信動作のフローチャートを示す。Ｓ５０１は制御変数ｓの初期化ステップ、Ｓ５０２はメッセージ送信ステップ、Ｓ５０３は確認応答受信タイムアウト判定ステップ、Ｓ５０４は確認応答受信ステップ、Ｓ５０５は制御変数ｗの初期化ステップ、Ｓ５０６はメッセージリリース時刻決定手続き、Ｓ５０７はリリース許可メッセージ送信手続き、Ｓ５０８はリリース許可確認応答受信タイムアウト判定手続き、Ｓ５０９はリリース許可確認応答受信手続き、Ｓ５１０は制御変数ｓの増加ステップ、Ｓ５１１は制御変数ｓの判定ステップ、Ｓ５１２はエラー処理、Ｓ５２０は制御変数ｗの増加ステップ、Ｓ５２１は制御変数２の判定ステップ、Ｓ５２２はエラー処理をそれぞれ表す。

【００５８】

図１３は認証サーバ２０を用いた構成を示す図である。１は同報送信装置、９０１は受信装置１、９０２は受信装置２である。

図１４にニュース配送と株式の自動取引を組み合わせたシステムの実施形態を示す。１００１は通信社、１００２はニュース配送システム、１００３は同報送信装置、１１０３は同報コネクション、１１０１－１～ｎは同報コネクション１１０３を通じて通信社からニュースを受信する証券投資システムをそれぞれ表す。送受信装置１１０２－１～ｎは証券投資システム１１０１－１～ｎに接続され同報の公平性を保証する装置を表す。

【００５９】

１２０１－１～ｍは証券会社側の証券取引システム、１２０２－１～ｍは対応する送受信装置、１２０３－１は顧客側の証券投資システムの送受信装置１１０２－１～ｎと証券会社側の証券取引きシステムの受信装置１２０２－１を接続する多対一接続型のコネクションである。

【００６０】

１２０１－１～ｍは各証券会社１～ｍの証券取引システム、１２０２－１～ｍはそれぞれの証券取引システムの受診装置、１２０３－１～ｍは各証券会社１～ｍと顧客を接続する多対一接続型のコネクションである。

【００６１】

１３０１は証券取引所、１２０４－１～ｍは証券取引所と各証券会社の証券取引システムを接続する専用線をそれぞれ表す。

以下、図１及び図２に従って本発明の一実施例の動作を説明する。

【００６２】

以下では、本発明を大きく３つの部分、すなわち受信装置が信頼できる装置であることをネットワークを通じて確認する手続き及び装置の構成と、受信装置においてメッセージのリリース時刻を一致させる手続き及び本発明の応用システムの３つに分けて順番に説明する。

【００６３】

以下メッセージという言葉は送信装置または受信プロトコル装置が、同位の送信装置との間またはメッセージ受信時刻を保証するプロトコル上位装置との間でやりとりする意味を持つ一つのデータ単位を表す。またパケットという言葉は送信装置または受信プロトコル装置が物理ネットワークに送出するデータのまとまりを意味する。本実施例では具体的にはＡＡＬ５のパケットを示す。メッセージはネットワークを伝送する際に一つまたは複数のパケットとして伝送される。

【００６４】

まず同報群の加入について説明する。同報群は予め定義された一意の同報群識別子を持ち、対応する同報送信装置のＥ．１６４アドレスとともに、例えば電話帳やディレクトリサービスによって公開され、知ることができる。

【００６５】
同報群の受信を行おうとするクライアント装置１１－１はまず同報群加入手続き１０１を実行する。図３に同報群加入手続き１０１のより詳細なフローチャートを示す。まず受信装置は同報送信装置１との間にポイント－ポイントのコネクションを設定し、同報群加入手続きを開始するステップ１０２を実行する。クライアント装置１１－１は、加入する同報群の識別子と対応する同報送信装置のＥ．１６４アドレスを含む同報群加入セットアップ要求を準備し、上位インタフェース１４－１を通じて１２－１受信プロトコル装置に引き渡す。

【００６６】
受信プロトコル装置は、クライアント装置から渡されたメッセージが同報群加入要求である場合、図９における３０９コネクション設定機能が、コネクション設定メッセージを１３－１～ｎは網側イナンタフェース装置に渡す。網側インタフェース装置はセットアップメッセージをシグナリングプロトコルに従って通信網３１に送信する。

【００６７】
クライアント装置１１－１は同報送信装置のＥ．１６４アドレスから同報送信装置へのコネクションセットアップメッセージを生成する。このメッセージには同報群を示す識別子が含まれ、１６－１網側インタフェース点から通信網３１に向けて送出される。このメッセージ形式はＡＴＭインタフェース仕様（ＡＴＭ　ｆｏｒｕｍ　ＵＮＩ　３．１　仕様，ＴｈｅＡＴＭ　Ｆｏｒｕｍ，１９９４）の定められたものに、同報群を示す識別子を付加したものとする。

【００６８】
このセットアップメッセージによって、通信網３１に受信プロトコル装置１２－１と同報送信装置１の間のポイント－ポイントのコネクション３２－１が設定される。同時にセットアップメッセージに含まれる同報群識別子が同報送信装置１に渡され、同報送信装置１は図１０の同報群加入手続きＳ４２１を開始する。

【００６９】
次に同報送信装置１はポイント－ポイントコネクション３２－１を通じて同報受信プロトコル装置１２－１が持つ識別子１７が同報送信装置１のもつ識別子テーブル２に存在するかどうかを認識する。これは同報送信装置１では図１１のステップＳ４２２、受信プロトコル装置１２－１では図３のステップＳ１０３に相当する。

【００７０】
各同報受信プロトコル装置１２－１～ｎは予め信頼できる公的な機関によって製造出荷時にそのプロトコル実装が正当なものであることが保証され、その証として付与された秘密の受信プロトコル装置識別子１７を格納している。識別子１７は公的な機関がこの識別子の値は装置が正当であることを証明するものであるため、値が不正に使用されることを防ぐために、この値が上位インタフェース１４及び下位インタフェース１５から直接読み出されないように保護されている。

【００７１】
更に、受信プロトコル装置の装置識別子１７が不正に読み出されることを防ぐために、装置の筐体には破壊を検出する機能が備えられる。識別子はＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍａｂｌｅ　ＲＯＭ）に記憶され、筐体の破壊が検出されると消去される。このような技術は既に知られている。（Ｍｏｒｉ，Ｒ．，Ｋａｗａｈａｒａ，Ｍ：”Ｓｕｐｅｒｄｉｓｔｒｉｂｕｔｉｏｎ：Ｔｈｅ Ｃｏｎｃｅｐｔ ａｎｄ Ａｒｃｈｉｔｅｃｔｕｒｅ”，ＩＥＩＣＥ ｔｒａｎｓａｃｔｉｏｎ ７３（７），１９９０）。

【００７２】
同報送信装置１は予め正しいプロトコル実装を持つことが公的な機関によって保証された受信装置識別子テーブル２を持つ。このテーブルは信頼できる機関によって管理される。

【００７３】
受信プロトコル装置は直接に装置識別子をネットワーク上のメッセージの一部として含む

ことなく通信によって同報送信装置１に装置識別子を持つことを証明し、そのプロトコル処理の実装が正当なものであることの証しとする。これは、通信の傍受によって装置識別子を盗まれることや、受信装置を認証する送信装置とは別な装置が送信装置を偽って装置識別子を盗むことを防ぐためである。

【００７４】

このようなプロトコルはいわゆるゼロ知識証明として良く知られている。代表的なアルゴリズムにＦｉａｔとＳｈａｍｉｒのものがある（Ｆｉａｔ，Ａ．，Ｓｈａｍｉｒ，Ａ．：”Ｈｏｗ ｔｏ ｐｒｏｖｅ ｙｏｕｒｓｅｌｆ：ｐｒａｃｔｉｃａｌ ｓｏｌｕｔｉｏｎ ｔｏ ｉｄｅｎｔｉｆｉｃａｔｉｏｎ ａｎｄ ｓｉｇｎａｔｕｒｅ ｐｒｏｂｌｅｍｓ”，Ｐｒｏｃ．ｏｆ ＣＲＹＰＴＯ ８６，Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ，Ｂｅｒｌｉｎ，１９８７）。

【００７５】

本実施形態では前記ＦｉａｔとＳｈａｍｉｒのアルゴリズムに基づき、受信プロトコル装置は装置識別子ｓと大きな整数ｎを持っている。一方受信プロトコル装置の識別子テーブル２には装置識別子ｓの法ｎにおける２乗ｖ：ｓ＝ｖ^2　（ｍｏｄ　ｎ）が格納されている。

【００７６】

同報送信装置は受信プロトコル装置がｓを持っていることをゼロ知識証明の方法によって確認し、また証明のために得た値ｖ：ｓ＝ｖ^2　（ｍｏｄ　ｎ）が確かに受信ブロトコル装置の識別子テーブル２に存在することを確かめ、その識別子が信頼できる機関によって与えられたものであることを確認する。ｎの因数分解が困難である限り、ｖ：ｓ＝ｖ^2　（ｍｏｄ　ｎ）が知られてもｓを知ることは困難なため、ｓは安全である。

【００７７】

各送信装置が受信装置識別子テーブル２を待たず、図１３に示すように受信装置識別子テーブル２を持つ認証サーバ２０に問い合わせを行うことで認証を行っても良い。同報送信装置は認証の実行にあたっては認証サーバと受信装置のメッセージのやりとりを中継し、最終的な認証の結果をサーバから得る。この方式をとれば各送信装置が受信装置識別子テーブルを持つ必要がない。

【００７８】

次に受信装置で、同報送信装置１と受信プロトコル装置１２の間の秘密鍵を共有するステップＳ１０４が実行される。送信装置ではステップＳ４２３に対応する。この手順についても良く知られた方法が存在する（Ｄｉｆｆｉｅ，Ｗ．，Ｈｅｌｌｍａｎ，Ｈ．：”Ｎｅｗ ｄｉｒｅｃｔｉｏｎｓ ｉｎ ｃｒｙｐｔｏｇｒａｐｈｙ” ＩＥＥＥ ｔｒａｎｓａｃｔｒｉｏｎ ｏｆ ｉｎｆｏｒｍａｔｉｏｎ ｔｈｅｏｒｙ ６：６４４－６４５，１９７６）。この方法では送信装置と受信装置との間で予め十分大きな素数ｐとＧＦ（ｐ）上の原子根αを共有していることが必要である。これらの値は公開しても安全なので、同報送信装置がこのステップの実行の始めにこれらの値を受信プロトコル装置に転送する。

【００７９】

ステップＳ１０３までを正規の識別子が与えられた受信プロトコル装置が行い、その直後の秘密鍵共有手順Ｓ１０４からを不正な装置で行うなりすましの攻撃が考えられる。これを防ぐために、同報送信装置１はステップＳ１０３で受信プロトコル装置が正規な識別子を持つことが確認できた後の秘密鍵共有ステップ１０４においても受信プロトコル装置が正規な識別子を持つ認証を続けることが望ましい。

【００８０】

以後、秘密鍵共有手段１０４及び４２３が終了して同報送信装置１と受信プロトコル装置１２－１との間の共通秘密鍵Ｋ１　が生成できた後は受信プロトコル装置は秘密鍵Ｋ１を用いて送信メッセージに認証子を付加し、メッセージの攻竄及びなりすましを防ぐ。同報送信装置は共通鍵を用いてメッセージに付加された認証子を検査し、不正が認められた場合はそのパケットを廃棄する。

【００８１】
次に同報送信装置はこの秘密鍵Ｋ１を用いて暗号化された同報送信メッセージの復号化鍵Ｋを受信プロトコル装置１２－１に送信し、受信プロトコル装置はそれを受信するステップＳ１０５を実行する。この場合の暗号化アルゴリズムは通常の秘密鍵暗号、例えばＤＥＳが使用できる。送信装置ではステップＳ４２４に対応する。
【００８２】
このような２段階の手段を踏むのは次の理由による。最初に共有化される鍵Ｋ１　は同報送信装置１と受信プロトコル装置１２－１の間でしか共通ではない。同じ同報群に属する他の受信プロトコル装置１２－２～１２－ｎは鍵Ｋ２　，…，Ｋｎをそれぞれ持つ。同報の暗号化を１つの鍵で行うためには、全ての受信プロトコル装置１２－１～ｎで共通の鍵を持つ必要がある。
【００８３】
以下に、同報送信装置１から見た同報群加入手続きを図１２に従って説明する。
同報送信装置１において、受信装置認証ステップＳ４２２は、受信プロトコル装置の識別子の照明ステップＳ１０３に対応し、受信プロトコル装置との鍵共有ステップＳ４２３は、受信プロトコル装置の送信装置との鍵共有ステップＳ１０４に対応し、同報群の鍵送信ステップＳ１０５は、受信プロトコル装置の同報群の鍵取得ステップＳ１０５にそれぞれ対応する。
【００８４】
同報送信装置１では、これらのステップを順次実行した後、図８における同報群管理機能２１２により、受信プロトコル装置１２－１を同報群に登録するステップ４２５が実行される。
【００８５】
図１における同報コネクション認定機能２１３を通じて同報コネクション３３に受信プロトコル装置１２－１が接続しているインタフェース装置１３－１を加える。この設定はステップＳ１０２で行われた同報群加入手続きで得られたインタフェース装置１３－１のＥ．１６４アドレスの情報を利用したシグナリング手続きで行われる。このステップＳ４２６で同報コネクションに受信プロトコル装置１２が加えられ、同報通信が開始される。
【００８６】
以上が端末の同報群への加入時に受信装置が信頼できる装置であることを示す手続きである。
次にメッセージの順序制御及びリリース時刻を一致させる手続きについて説明する。
【００８７】
本発明は同報群に含まれる全ての受信装置で同一の時刻にメッセージリリースを行うことを目的としている。メッセージリリース時刻を共有する方式には幾つかの方式がある。詳細については各実施例において説明するが、メッセージ本体の配送方法とリリース時刻の配送方法によって６通りの組合せがある。受信装置において、各方式で１メッセージの配送に必要な最低の処理パケット数との関係を図２７に示す。以下、各方式について説明する。ここではメッセージのリリース時刻を送信装置が決定することを例にとって説明しているが、リリース時刻決定の対象となるメッセージを送信した装置と決定したリリース時刻を通知する装置とは別であっても差し支えない。
【００８８】
まず‘メッセージ配送に確認あり’は、メッセージ本体が正しく各端末に配送されたことを確認し、その後に（送信装置が複数存在する場合はリリース順序）リリース時刻が決定され、各装置に通知される２ｐｈａｓｅの方式である。メッセージ本体を構成するパケット１パケット毎に確認応答が返されるので、メッセージ本体がｍ個のパケットで構成されていれば、本体の送信には最低２ｍ個のパケットが必要である。この方式はリリース時刻の通知及びその確認の方法によってさらに細かく分類される。どの方法でも予めあるリリース時刻通知の繰り返し数を定めてリリース時刻はその繰り返し時刻後に設定し、そのリリース時刻を通知するパケットを受信装置に繰り返し送信することにより、パケットの遅

延、紛失が生じる環境でも全ての受信装置が十分高い確率でリリース時刻の共有に成功するようにしていることが特徴である。

【００８９】

‘リリース時刻の確認応答あり’では、リリース時刻を通知するメッセージ毎に受信装置が確認応答を送信装置に返す。送信装置は確認応答を返さない端末にリリース時刻通知を再送する。また、確認応答を返さない、つまり受信に失敗した端末が多い場合はリリース時刻を遅らせる修正を行い、再度リリース時刻通知を送信することができる。

【００９０】

‘リリース時刻の確認あり’では、リリース時刻の通知は予め定められたある間隔をおいて繰り返し行われる。受信端末は一回毎の確認応答は行わず、代わりにメッセージをリリースした後に正しい時刻にメッセージをリリースしたことを送信装置に通知する。送信装置はこの通知に対して確認応答を行う。

【００９１】

‘リリース結果の確認なし’では、リリース結果の送信装置への確認は行わない。リリース時刻の一致に失敗した場合でも、送信装置はそれを知ることができない。

【００９２】

‘メッセージ配送に確認なし’では、メッセージ本体の配送とリリース時刻の配送を同時に行う方式である。これはメッセージが１パケットに収まるような短いメッセージに対して簡易な、特に他方式に比較して低遅延の時刻一致手段を提供するものである。この方式ではメッセージ本体の配送を確認しないため、複数の送信装置の間で送信時刻に基づくメッセージの順序制御はできないことに注意しなければならない。

【００９３】

‘リリース時刻の確認応答あり’の場合には、メッセージ転送のｐｈａｓｅを省略して、リリース時刻とメッセージの両方が含まれたパケットを送信する。‘確認あり’説明したように受信装置は確認応答を送信装置に返し、送信装置は確認応答を返さない端末にリリース時刻通知を再送する。メッセージを構成するパケットが増えた場合再送にともなうパケット数増加が大きいことに注意する必要がある。

【００９４】

‘リリース時刻の確認あり’では、リリース時刻の通知は予め定められたある間隔において繰り返し行われる。受信端末は一回毎の確認応答は行わず、代わりにメッセージをリリースした後に正しい時刻にメッセージをリリースしたことを送信装置に通知する。送信装置はこの通知に対して確認応答を行う。

【００９５】

‘リリース結果の確認なし’リリース結果の送信装置への確認は行わない。リリース時刻の一致に失敗した場合でも、送信装置はそれを知ることができない。次に同報メッセージの送信と受信について図４，図１２，図１４に従って説明する。図４は受信手続きのフローチャート、図１２は送信手続きのフローチャート、図５は同報通信のメッセージシーケンスである。

【００９６】

再送手順が必要な同報通信について、再送制御を行うための確認応答を減らすためのさまざまな試みが行われている。代表的なものに確認応答メッセージを送信メッセージに組み込んでパケット数を減らすピギーバックあるいはパケット紛失を検出した時のみ否定の確認応答を行うものがある（Ｔａｋｉｚａｗａ，Ｍ：”Ｃｌｕｓｔｅｒ ｃｏｎｔｒｏｌ ｐｒｏｔｏｃｏｌ ｆｏｒ Ｈｉｇｈｌｙ ｒｅｌｉａｂｌｅ ｂｒｏａｄｃａｓｔ ｃｏｍｍｕｎｉｃａｔｉｏｎ”，Ｐｒｏｃ．ｏｆ ｔｈｅ ＩＦＩＰ Ｃｏｎｆ．ｏｎ Ｄｉｓｔｒｉｂｕｔｅｄ Ｐｒｏｃｅｓｓｉｎｇ，１９８７；Ｉｎｔｅｒｎｅｔ ＲＦＣ１３０１ ＭＴＰ，１９９２；Ｍｅｌｌｉａｒ－Ｓｍｉｔｈ 他，”Ｒｅｌｉａｂｌｅ ｂｒｏａｄｃａｓｔ ｐｒｏｔｏｃｏｌ”，ＵＳＰ ５，２１６，６７５，１９９０）。

【００９７】

本実施例ではメッセージがクライアント装置に配送される時間を公平にすることを第一の目標としているため、同報メッセージ転送のパケット利用効率に関する議論は行わず、もっとも簡単なメッセージ単位の確認応答を行う方式（ハンドシェイク方式）を例にとって説明する。本実施例にピギーバックや否定の確認応答の手法を組み合わせることによってよりパケット数を減らすことが可能である。

【００９８】

詳細な説明の前に予め説明に用いる定数の定義について説明しておく。

ある装置ｉから別の装置ｊにパケットを転送する際の遅延時間t_{ij}がある時間T_dよりも大きな確率をＰ（$t_{ij}>T_d$）で表す。遅延時間の最大値をT_dとしたときそれを越えて遅延したパケットは紛失とみなすことができる。遅延時間の最大値をT_dとしたとき$P_{loss.ij}=P(t_{ij}>T_d)$を装置ｉから装置ｊへのメッセージ紛失確率とする。

【００９９】

同様にT_dを与えた時、同報群を構成する任意の装置の組合せについて単一パケットあたりの紛失確率の最大値を$P_{loss}(T_d)=max\{P_{loss.ij}\}$と定義する。逆に紛失確率を$P_{loss}$と与えた時、それに見合う遅延時間の最大値（$T_{max}$）を求めることができる。

【０１００】

また、装置ｉから装置ｊへメッセージが送られ、そこで処理時間T_Pの処理を行って応答が返るまでの時間RTT_{ij}は、ｉからｊへの転送時間をt_{ij}，ｊからｉへの転送時間をt_{ji}とすると、$RTT_{ij}=t_{ij}+T_P+t_{ji}$であり、これがＰ（$RTT_{ij}>T$）なる分布をするものとする。あるタイムアウト確率$P_{tout}$を定義した時、$P_{tout}>P(RTT_{ij}>T_s)$となるように$T_s$を定める。

【０１０１】

上に定義したパケット毎の紛失確率$P_{loss}(T_d)$は十分に大きな時間間隔をとって送信されたパケットの紛失確率にはよくあてはまる。しかし、連続して、または近い間隔で送信されたパケットの紛失確率はそれぞれ独立ではないと考えられる。これはネットワークで発生するエラーはある時間内に集中する傾向があるためである。例えばネットワークの輻輳によるＡＴＭセルの紛失や、経路制御の不具合や伝送リンクの経路切替えによるビットエラーによって連続したパケットにエラーが生じる可能性がある。この現象を以下バーストエラーと呼ぶ。

【０１０２】

あるバーストエラー状態が継続する期間がパラメータＴより長い確率分布を$P_{Burst.ij}(T)$とし、P_{loss}と同様にその最大値を$P_{Burst}(T_i)$とする。バーストエラーが存在する時、２つのパケットが短い時間に連続して送出されれば単一のバーストエラーによってともに失われてしまう可能性があるが、パケットを複数回送信するときにバーストの期間よりも長い間隔をおけばそれを避けることができる。

【０１０３】

$P_{Burst}(T_i)<P_{loss}(T)$となるようにパケットの送信間隔$T_i$を定めることによって個々のメッセージの紛失確率は独立でその値は最大でもP_{loss}とみなすことができる。

【０１０４】

受信装置の処理能力によって変わる定数として、リリースメッセージまたはメッセージとリリース時刻が含まれたメッセージを受信してからメッセージを上位処理装置にリリースできるようになるまでの所要時間をT_{dec}とする。

【０１０５】

図２８に定数の定義をまとめる。

はじめに‘メッセージ配送の確認あり’、‘リリース時刻の確認応答あり’の実施例を説明する。

【０１０６】

メッセージの送信シーケンスは、同報送信装置がメッセージM_1　を同報コネクションに送信することから始まる。メッセージには次の情報が含まれる。
・同報メッセージ本体
・メッセージ種別＝メッセージ
・同報メッセージ識別子
・メッセージ認証子
同報メッセージ本体は同報メッセージ入力機能２０２から同報プロトコル管理機能２０３に入力されたメッセージ、または制御情報が含まれる。メッセージ種別は当該メッセージがメッセージを含むのか制御情報を含むのかを示す。同報メッセージ識別子はメッセージの順序を示す通し番号で、十分長い周期を持つ。

【０１０７】
メッセージ認証子はこれらのメッセージが改竄されていないことを確認するための認証子である。メッセージ認証子を除くメッセージ、すなわち暗号化される前の同報メッセージ本体、同報メッセージ型識別子、同報メッセージ識別子を同報のための秘密鍵Ｋにより予め定められた符号化方式例えばＭＤ５とＤＥＳを組合せた符号化方式（Ｊ．Ｋｏｈｌ，“ＲＦＣ１５１０：Ｔｈｅ　Ｋｅｒｂｅｒｏｓ　Ｎｅｔｗｏｒｋｓ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｓｅｒｖｉｃｅ”，１９９３）によって符号化した値を用いる。同報通信の認証に用いられるメッセージ認証子の鍵は、同報群共通の鍵Ｋを使うため、鍵配送メッセージの認証子とは別のものであることを注意しなければならない。認証子の符号化方式自体は同じものでも構わない。

【０１０８】
これらのフィールドは全て暗号化機能２０４によって鍵Ｋで暗号化されて同報される。受信側では鍵Ｋを用いてメッセージの対応部分の認証子を計算し、その値が一致すればメッセージ及びプロトコル情報は改竄されていないと判断し続く処理を行う。以下の説明では送信時の認証子の付加及び受信時の認証子の検査は省略する。認証子を持たない場合、メッセージの一部、例えば特定のメッセージ識別子の値に対応する暗号と対応するメッセージ上の位置を知れば、当該部分のみを入れ換えることによってプロトコル情報などを改竄することができる。だがメッセージ全体についての情報と鍵情報を持たない限り知ることのできない情報すなわち認証子を含むことによってメッセージの部分的な改竄を検出することができる。

【０１０９】
ステップ５０１でメッセージ送信前に同報送信装置はメッセージの識別子ｐをｐ－ｐ＋１として一つ増分する。そしてメッセージＰの制御変数ｓを０に初期化する。制御変数ｓはメッセージ毎に区別されるがここでは煩雑さを避けるため単にｓと表記する。

【０１１０】
図１２のステップ５０２で同報送信装置は識別子番号ｐ、メッセージ型＝メッセージを持つメッセージM_p　を同報する。同報送信装置は同時にタイマＴ１　を現在時刻からT_s　後に設定する。

【０１１１】
受信プロトコル装置は図４のステップ１２２で上記識別子番号M_p　を持つメッセージを受信し、送信側のｓと同様に制御変数ｊを０に設定する。次に確認応答ACK_p　（Ａ）をマスタに送信する。これがステップ１２３である。

【０１１２】
確認応答ACK_p　（Ａ）には少なくとも次の情報が含まれ、送信メッセージと同様に鍵Ｋで暗号化される。メッセージには少なくとも次の情報が含まれる。
・メッセージ種別＝確認
・メッセージ識別子
・受信装置識別子
・メッセージ認証子
送信装置はステップ５０４で確認応答の受信を行う。識別子ｐのメッセージについて、同

報群全ての確認応答が受信できれば次のステップ５０５を実行する。タイマＴ１ に設定した時刻までに全ての確認応答が受信できなければ、送信装置はタイムアウトと判定する。これがステップ５０３である。制御変数ｓが予め定められた値S_{max} 以下であるかの判定を行い（ステップ５１１）、ＳがS_{max} 以下であればＳの値を１増加して（ステップ５１０）、メッセージの再送を行う。

【０１１３】

受信側はメッセージ識別子によって受信済みと判断されるメッセージを受信した場合にも再度確認応答を送信する。これは受信側でメッセージの受信には成功していても、確認応答が紛失することによって送信側では受信に失敗したと判断している場合があるためである。送信側において、確認応答がタイムアウトする確率はタイムＴ１ がT_s であることから、P_{tout}以下となる。S_{max} 回の送信がすべての失敗してある端末がメッセージを受信できない確率は（P_{tout}）S_{max} である。端末数をｎ台としたとき１台以上の端末で受信に失敗する確率は（１－（P_{tout}）S_{max} ）^{n} となる。従って、S_{max} を増やすことにより失敗する確率を任意に低くすることができる。ただし、S_{max} を増やすことメッセージ配送の遅延時間を増やすことになり、両者はトレードオフの関係にある。図２０にP_{loss}＝１０$^{-3}$ の場合にｎ＝３，５，１０，１０００について再送回数とメッセージが一回も受けとれないノードがある確率をプロットした図を示す。メッセージ紛失確率が１０$^{-3}$ でノード数が１０００の時に配送失敗の確率を１０$^{-12}$ 以下が要求されれば、再送回数を５回以上にすればよい。

【０１１４】

ｓがS_{max} を越えた場合、エラー処理ステップ５１２が実行される。エラー処理には、当該メッセージの送信を失敗とする方法と、確認応答の得られなかった装置を故障と判断して同報群からの切り離し操作を行う方法の２通りが考えられる。これらについては後に詳しく述べる。

【０１１５】

次にエラー処理と上位アプリケーションの関係について述べる。エラーが生じた場合の対処法には３通りある。

・上位にエラー発生を通知して同報群は維持する。

【０１１６】

電子会議システムの資料配布

・受信に失敗した端末を同報群から切り離して同報群は維持。

ニュース配送

・同報群の同報通信を終了。

【０１１７】

アプリケーションの中止。銀行口座の分散管理システム

全ての装置から確認応答が受信できた後の処理ステップ５０５では制御変数ｗを０に初期化する。当該メッセージより若い識別番号を持つ末リリースのメッセージがあれば、末リリースメッセージの時刻のリリース時刻通知が完了するまでリリース時刻の決定を待つ。待ち状態が終了するとステップ５０６で当該メッセージのリリース時刻を設定する。リリース時刻は次のように決定する。

【０１１８】

受信装置がリリースメッセージを受信してから上位装置にパケットを出力できるようになるまでの所要時間をt_{dec} ，最大再送回数をW_{max} とする。確認応答のタイムアウト時間をT_s 、リリースメッセージ送信の時刻をＴとするとメッセージのリリース時刻T_r は、次の式で表される。

【０１１９】

T_r （ｐ）＝Ｔ＋W_{max} ・T_s ＋t_{dec}

W_{max} はメッセージの場合と同様に、（１－（P_{tout}）W_{max} ）^{n} が時刻配送の失敗確率の許容値をしたまわるように定める。ここでタイムアウト時間T_s はバーストエラー時間を回避できるバケット送出間隔T_i よりも大きい、すなわちT_s ＞

t_i の関係が成り立つものとする。もしT_s ＜t_i ならば、以下の説明で用いるタイムＴ３の設定値T_i とする。以上の方法によりメッセージのリリース時刻を定めれば、リリース順序はリリースメッセージ発行時刻Ｔの順序となり、メッセージのリリース順序は正しく守られる。

【０１２０】

時刻決定の際に、次に説明する受信装置のクライアント装置へのメッセージを出力する際のスケジューリング条件を加えても良い。受信装置で複数の同報通信を収容している場合、それぞれの同報群が上位インタフェースやメッセージ復号化機能などの資源の利用をめぐって競合することがある。この競合を避けるため、図４ステップ１２３の確認応答送信の際にどの時点が利用可能であるかを表す情報を確認応答メッセージに付加し、その情報に基づいて同報群全ての受信プロトコル装置で十分な資源割当が可能でクライアント装置にメッセージを出力できる時刻をメッセージリリース予定時刻として設定すれば、複数の同報群を扱う場合にも全ての受信プロトコル装置でリリース時刻を保証することが可能である。送信装置は確認応答受信ステップ５０４でスケジューリング情報を取得する。この場合にはメッセージのリリース順序が逆転しないようにリリース時刻を選ぶ必要がある。

【０１２１】

スケジューリング条件を考慮する場合、確認応答メッセージには少なくとも次の情報が含まれる。

・メッセージ種別＝確認応答
・メッセージ識別子
・受信装置識別子
・メッセージスケジューリング情報
・メッセージ認証子

受信時刻を決定すると、送信装置はリリース許可メッセージREL_p （ｉ） を同報する。ｐは対応する送信メッセージ、ｉはリリース許可メッセージの識別子である。リリース許可メッセージは少なくとも次の情報を含む。

【０１２２】

・メッセージ種別＝リリース
・メッセージ識別子
・リリースメッセージ識別子
・メッセージリリース予定時刻＝T_r （ｉ）
・メッセージ認証子

リリース許可メッセージの送信と同時に送信装置はタイマＴ３を現在時刻からＴｓ 後に設定する。これがステップ５０７である。

【０１２３】

受信装置ではステップ１２５でリリース許可メッセージREL_p （０） を受信する。タイマＴ２がタイムアウトするまでリリース許可メッセージが受信できない場合の処理ステップ１３１，１３０，１３２は送信側における確認応答のタイムアウトの処理と同様である。

【０１２４】

リリース許可を受信すると、受信装置はステップ１２６を実行してリリース許可確認応答$RACK_p$ （ｉ，Ａ）を送信装置に送信する。ここでｉはリリースメッセージ識別子，Ａは受信装置識別子である。そしてタイマＴ４をリリース許可メッセージに含まれるリリース予定時刻に設定する。

【０１２５】

リリース許可確認応答は少なくとも次の情報を含む。

・メッセージ種別＝リリース確認
・メッセージ識別子
・リリースメッセージ識別子
・受信装置識別子

・メッセージ認証子
これらに加えてリリース許可確認応答にリリース許可確認応答受信失敗に備えて更新されたメッセージスケジューリング情報を付加しても良い。この場合、受信装置はステップ１２６で再びスケジューリング情報の取得を行い、リリース許可確認応答を送信する。
【０１２６】
さて、送信装置はタイマＴ３のタイムアウトまでに全ての受診装置からのリリース許可確認応答を受信すれば、送信処理を正常に終了する。
受信装置では、ステップ１２７でタイマＴ４のタイムアウト時刻すなわちリリース時刻迄に送信装置から再度当該メッセージのリリース許可REL_p（ｉ＋１）を受信しなければ、ステップ１４０を実行してリリース時刻ＴＲ（ｉ）に復号化したメッセージを上位インタフェースを通じてクライアント装置に出力する。これでメッセージｐの受信は終了する。
【０１２７】
メッセージの復号化はリリース時刻に間に合う限り、最初にメッセージを受信した時点からメッセージ出力までのいつ行っても良い。この順序に合わせて図９のメッセージ復号手段３０３とメッセージ蓄積手段３０４の配置も変更しなければならない。
【０１２８】
受信装置がリリース許可確認応答を行う第一の目的は送信装置がリリース許可メッセージの選択再送を行い無駄な再送を減らすことである。もう一つ確認応答を行うことによって受信装置がどれだけリリース許可メッセージを受信できているかを送信装置が知り、リリース許可を正しく受信できている装置が少ない場合にはリリース時刻を延期することができる。これは既にリリース許可を受信した受信装置に修正したリリース時刻を通知することによって行う。
【０１２９】
リリース時刻を延期する条件としては送信装置がW_{max}回の半分の回数の確認応答受信処理を完了した時点で予め定めらた割合、例えば半数以上の受信装置がリリース許可メッセージを受信出来ていない場合、とすることができる。この時点で修正したリリース時刻を通知すれば、既に古いリリース許可時刻を受信した受信装置もメッセージリリース時刻が至る前に修正されたメッセージリリース時刻を受信できることが期待できる。
【０１３０】
ただし、リリース時刻の修正を行う場合にはメッセージのリリース順序が逆転してしまう可能性が生じる。この問題は次の２つのいずれかの方法で解決できる。ひとつはリリース時刻が完全に確定するまで次のメッセージのリリース時刻を通知するのを待つ方法である。もう一つはあるメッセージのリリース時刻が修正されたら、それに続くメッセージのリリース時刻も修正する方法である。
【０１３１】
次に一つの同報群に複数の送信装置が存在する場合について説明する。複数の送信装置が存在する時、それらが送信するメッセージの受信順序を同報群で一致させるには従来の技術をそのまま使うことができる。受信順序確定後にこれまで説明した方法により、メッセージのリリース時刻を決定する方法は容易に類推可能である。図７に送信装置（センダ）が複数存在し、１台のマスタが受信順序を決定する場合のメッセージシーケンスを示す。ここではわかりやすさのため送信装置と受信装置を別に記述したが、送信装置と受信装置が同一のネットワークアドレスを持つ、あるいは同一の筐体に格納され、装置の認証も一括して行う方式を取っても良い。加入手続きは同報群に１台だけ存在するマスタに対して行われ、同報群のメンバや鍵の管理はマスタが集中して行う。
【０１３２】
ここでは従来技術で問題となっていた不正プロトコル動作による受信順序の操作は、プロトコルの動作が正しいことが装置の認証により保証されているため発生しない。
【０１３３】
また、公平性の確保のため、メッセージの受信順序に送信装置のメッセージ送信時刻を反

映させることが要求される場合、受信順序の決定を送信メッセージに付化された絶対時刻によって行っても良い。

【０１３４】

次に、受信者の同報群からの離脱について説明する。ある受信装置が同報群から離脱した時、その装置は同報の復号化鍵を持っているため、復号化鍵を変更しなければならない。

【０１３５】

次に、暗号の変更について説明する。変更した鍵の配布はそれぞれの受信装置毎のコネクションを通じて、受信装置毎の鍵配布用の鍵を用いた暗号化メッセージをすることによって行う。これは図１０のステップ４３１，４４１に相当する。

【０１３６】

時刻同期の方法は既にさまざまなものが知られている。例えば主にパケット交換網であるインターネットにおける標準としては、「Ｍｉｌｌｓ，Ｄ．Ｌ．：”Ｎｅｔｗｏｒｋ　Ｔｉｍｅ　Ｐｒｏｔｏｃｏｌ”；ＩＥＴＦ　ＲＦＣ１０５９，１９８８」が知られている。また、公衆網に接続された物理回線のフレーム周期は原子時計と周期しているため極めて正確であり、時刻同期に利用すれば高い精度を得ることができる。また、対タンパーな装置内部にＧＰＳ（Ｇｌｏｂａｌ　Ｐｏｓｉｔｉｏｎｉｎｇ　Ｓｙｓｔｅｍ）の受信装置を置くことによって正しい時刻を得ることも可能である。

【０１３７】

時刻周期は同報通信の開始前に精度の要求を満たすように同期を取っておき、同報通信を継続中にも常に同期を取ることが望ましい。

次に、リリース時刻計算のペナルティについて説明する。ある同報に対する応答の順序が重要な意味を持つ場合がある。例えば入札などである。このようなアプリケーションに対しては、配送時刻を同一とするのではなく、応答の遅延時間を保証するようなメッセージのリリース時刻を設定することによって公平性を確保することができる。

【０１３８】

次に、故障履歴の保存について説明する。本発明の装置は電子商取り引きなどのメッセージ配送時刻について高度の公平性が要求される分野に適合するが、実用かされた場合、装置の故障が与える影響は大きい。

【０１３９】

例えば株の売買に本発明の装置を利用している場合、装置の故障により取り引きできなければ、利用者は多大な損害を被ることが考えられる。網側の故障によっても同様の事態は生じる。

【０１４０】

装置の自己診断の結果を装置内に格納しておき、信頼できる第三者がそれを検査して装置の故障があったと判断すれば、故障が原因で生じた損害については保検機関が保証することによって本発明の装置をより安全に運用することができる。もちろん故障情報は利用者が書き換えることはできない。

【０１４１】

また、公衆網の故障については公衆網から故障情報を受けとり、装置内部に保存することによって網側の故障を証明することができる。故障情報の転送はＡＴＭではＯＡＭセルや物理レイヤのフレームのオーバヘッド情報を用いることができる。網側は故障装置、時刻などの情報を暗号化して提供することに故障情報の偽造を防ぐことができる。

【０１４２】

逆に故意に装置を動作不能な状況、例えば電源断、回線切り離しなどの状況においていたことが装置と網側の記録を照合することによりわかるため、網サービスのベンダは不正にサービスの利用不可能によって生じた損害の保証を要求されることはない。もちろん全ての故障を検出、記録することは不可能だが、検出可能な故障についてこれらの方法を組み合わせることにより、故障責任を明確化し、利用者の負担を減らすことができる。

【０１４３】

（実施例２）

実施例１においては同報群の全ての受信装置でメッセージの転送が成功したことを確認し、メッセージ順序を考慮してリリース時刻を受信装置に配布する手順をとっていた。

【０１４４】

実施例２ではメッセージが十分小さく、メッセージ本体とリリース指定時刻を単一のパケットに格納可能できる場合の簡易な時刻保証の手順を説明する。これは表１に示したメッセージ配送方式の分類の中で‘メッセージ配送に確認なし’，‘リリース結果の確認なし’に対応する。この実施例の目的は、ある送信装置から送信されたメッセージについて、各受信装置のメッセージ受信時刻を一致させることのみである。複数の送信装置の間で送信時刻に基づくメッセージの順序制御は行わないが、各受信装置で受信時刻が一致するため、結果としてメッセージの順序の一致が保証される。ただし複数の送信装置からの同一のリリース時刻が指定されたメッセージが届いた時、それがどのように扱われるかはそれぞれの受信装置の処理依存となることに注意しなければならない。

【０１４５】

送信装置から送信されるメッセージには次の情報を含む。

・メッセージ本体
・メッセージ種別＝メッセージ
・リリース時刻
・同報メッセージ識別子
・メッセージ認証子

本実施例ではこのメッセージを複数回送信することにより、受信側でメッセージを正しく受けとり、そして複数回送られたうちのどのメッセージを受信した場合でも指定のリリース時刻にメッセージがリリースできるだけの余裕をもってリリース時刻を指定しておくことにより各受信装置で同一時刻にメッセージをリリースできるようにする。

【０１４６】

定数の定義は実施例１，表２に示したものと同様である。定数として、遅延時間をt_dとおいたときの同報群の最大メッセージ紛失確率$P_{loss}(t_d)$，装置ｉｊ間のタイムアウト時間をT_s、バーストによる紛失確率をP_{loss}としたときのパケット送出間隔t_i　リリース処理時間t_{dec}を使用する。

【０１４７】

メッセージのリリース時刻はT_rはメッセージ送出時の時刻をＴとして次のように定める。

$$T_r = T + t_r = t_i \cdot k + t_d + t_{dec}$$

受信側ではメッセージ受信後復号化手順を実行した後、リリース指定時刻T_rにメッセージをリリースする。確認応答は行わない。

【０１４８】

図２１に本実施例のメッセージ送信手続き、図２２にメッセージ受信手続き、図２３にメッセージシーケンスを示す。

（実施例３）

確認応答あり　実施例２ではメッセージ本体とリリース時刻を一つのメッセージとして送ることにより簡略な時刻一致を実現していた。だが、実施例２の方法では端末が受信に成功したか否かを送信装置は知るとができなかった。実施例３は受信装置がメッセージのリリース後に結果を送信装置に返すことにより、送信装置が受信結果を知ることができるようにしたものである。これは表１の分類で‘メッセージ配送に確認なし’，‘リリース結果の確認あり’に相当する。

【０１４９】

メッセージ送信手続きを図２４に、図２５にメッセージ受信手続き、図２６にメッセージシーケンスを示す。

指定時刻にメッセージをリリースした受信装置は確認応答メッセージを送信装置に送出する。

【０１５０】

確認応答メッセージには少なくとも次の情報が含まれる。
・メッセージ識別子
・メッセージ種別＝確認
・受信装置識別子
・メッセージ認証子
受信装置から確認応答を受信した送信装置は確認応答受信テーブルの当該受信装置のエントリに受信済みを記録し、確認応答受信済みメッセージを受信装置に送出する。
【０１５１】
確認応答受信済みメッセージには少なくとも次の情報が含まれる。
・メッセージ識別子
・メッセージ種別＝確認応答受信済み
・メッセージ認証子
受信装置は送信装置から当該メッセージに関する確認応答受信済みメッセージを受信すると、当該メッセージに関する確認応答送出動作を完了する。もし確認応答が受信できない場合は間隔T_sをおいて予め定められた再試行回数W_{max}まで再試行を行う。パラメータW_{max}の定め方は実施例１に説明した通りである。
【０１５２】
以上実施例１から３において、メッセージリリース時刻一致の手順について、図２７に示した６通りの組み合せのうち、３通りを具体的に説明した。残りの３通りの組合せについては以上の説明から容易に類推可能であり、ここでの説明は省略する。
【０１５３】
本発明を応用したより具体的な実施例である実施例４を図１４にしたがって説明する。図１４において、１００１は通信社、１００２はニュース配送システム、１００３は同報送信装置、１１０３は同報コネクション、１１０１－１～ｎは同報コネクション１１０３を通じて通信社からニュースを受信する証券投資システムをそれぞれ表す。送受信装置１１０２－１～ｎは証券投資システム１１０１－１～ｎに接続され、同報の公平性を保証する装置を表す。
【０１５４】
１２０１－１～ｍは証券会社側の証券取引システム、１２０２－１～ｍは対応する送受信装置、１２０３－１は顧客側の証券投資システムの送受信装置１１０２－１～ｎと証券会社側の証券取引システムの受信装置１２０２－１を接続する多対一接続型のコネクションである。１２０１－１～ｍは各証券会社１～ｍの証券取引システム、１２０２－１～ｍはそれぞれの証券取引システムの受信装置、１２０３－１～ｍは各証券会社１～ｍと顧客を接続する多対一接続型のコネクションである。１３０１は証券取引所、１２０４－１～ｍは証券取引所と各証券会社の証券取引システムを接続する専用線をそれぞれ表す。
【０１５５】
通信社からは株式市況に影響する可能性のある情報を顧客に配送するサービスを提供している。情報には、例えば公的な機関による雇用統計、住宅着工数、為替レートなどの情報、国際紛争の発生などがある。
【０１５６】
情報は同報送信装置１００３から各顧客の受信装置１１０２－１～ｎに公平かつ公正に配送される。従って、全ての顧客の証券投資システム１１０１－１～ｎは同時に情報を受信する。システムは着信した情報に基づいて投資を決定し、証券会社へ発注する。発注は多対一通信路１２０３－１を通じて証券会社の証券取引システム１２０１－１に送られる。この時、送信メッセージには絶対時刻が付加され、証券会社ではその時刻に基づいて先着した注文を優先して処理する。各証券会社と証券取引所の間は専用線１２０４－１～ｍで接続され、取引が行われる。
【０１５７】
同時性と時間順序が保証されるため、全ての顧客は伝送遅延や再送の発生に影響されることなく通信社からのメッセージを受けとることができる。また、証券会社への発注におい

ては送信時の時刻に基づいた順序で処理されるため、ここでも伝送遅延や再送に影響されることはない。この仕組みにより、距離や通信網の違いを越えて多くの顧客に公平な商機が与えられる。

【０１５８】

以下では、本発明を大きく３つの部分、すなわち受信装置が信頼できる装置であることをネットワークを通じて確認する手続き及び装置の構成と、受信装置においてメッセージのリリース時刻を一致させる手続き及び本発明の応用システムの３つに分けて順番に説明する。

【０１５９】

同時性と時間順序が保証されるため、全ての顧客は伝送遅延や再送の発生に影響されることなく通信社からのメッセージを受けとることができる。また、証券会社への発注においては送信時の時刻に基づいた順序で処理されるため、ここでも伝送遅延や再送に影響されることはない。この仕組みにより、距離や通信網の違いを越えて多くの顧客に公平な商機が与えられる。

【０１６０】

【発明の効果】

本発明によれば、伝送遅延に差のある場所においても公平な通信サービスが受けられるようになる。また、プロトコル違反による不正の可能性を排除できるため、公正な取り引きが実現できる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る送受信プロトコル装置の基本構成を示す図である。

【図２】受信プロトコル装置の動作の概略を示すフローチャートである。

【図３】受信プロトコル装置の同報群加入手続きＳ１０１の詳細を示すフローチャートである。

【図４】受信プロトコル装置の同報メッセージ受信手続きＳ１１１の詳細を示すフローチャートである。

【図５】同報メッセージ受信手続きの正常時のメッセージシーケンスを示す図である。

【図６】同報メッセージ受信手続きのメッセージリリース許可の転送失敗時のメッセージシーケンスを示す図である。

【図７】複数の送信者のメッセージ順序の合意を得る同報メッセージシーケンスを示す図である。

【図８】同報送信装置の機能ブロック図である。

【図９】同報受信プロトコル装置の機能ブロック図である。

【図１０】同報送信装置の同報群管理動作の概略を示すのフローチャートである。

【図１１】同報送信装置の同報群加入要求受け付け動作Ｓ４２１の詳細を示すフローチャートである。

【図１２】同報送信装置の同報送信動作を示すフローチャートである。

【図１３】認証サーバを使った本実施形態の構成を示す図である。

【図１４】ニュース配送と株式の自動取引を組み合わせたシステムの構成を示す図である。

【図１５】従来技術の同報メッセージシーケンスを示す図である。

【図１６】従来技術のメッセージ消失が起きた時の同報メッセージシーケンスを示す図である。

【図１７】従来技術でリリース許可メッセージ消失が起きた時の同報メッセージシーケンスを示す図である。

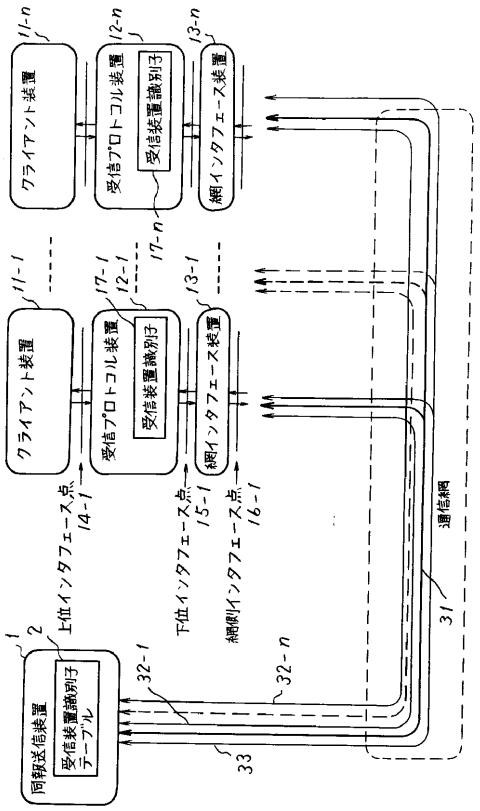
【図１８】従来技術でリリース許可メッセージ消失が起きた時の同報メッセージシーケンスを示す図である。

【図１９】従来技術で複数の送信者のメッセージ順序の合意を得る同報メッセージシーケンスを示す図である。

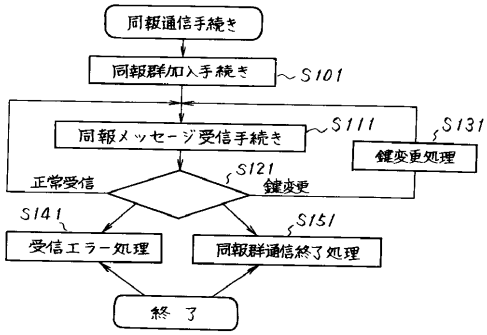
【図２０】エラー確率、端末数、及び再送の回数とメッセージ受信成功の確率の関係を表

すグラフである。
【図２１】実施例２のメッセージ送信手続きのフローチャートである。Ｓ２１０１は同報メッセージの送信手続き、Ｓ２１０２はT_i　時間の遅延、Ｓ２１０３はｋ回の繰り返し手続きをそれぞれ表す。
【図２２】実施例２のメッセージ受信手続きのフローチャートである。Ｓ２２０１はリリース時刻判定手続き、Ｓ２２０２は受信メッセージの有無判定手続き、Ｓ２２０３は受信メッセージの重複判定手続き、Ｓ２２０４はリリース予定リストへの追加手続き、Ｓ２２０５はメッセージの復号化手続き、Ｓ２２０６は受信メッセージ廃棄手続き、Ｓ２２０７はメッセージリリース手続をそれぞれ表す。
【図２３】実施例２のメッセージシーケンスである。２３０１は送信装置、２３０２は受信装置をそれぞれ表す。
【図２４】実施例３のメッセージ送信手続きのフローチャートである。Ｓ２４０１は同報メッセージ送出手続き、Ｓ２４０２はT_i　時間の待ち、Ｓ２４０３はｋ回の繰り返し手続き、Ｓ２４０４は確認応答判定手続き、Ｓ２４０５はタイムアウト判定手続き、Ｓ２４０６は受信失敗装置確定手続き、Ｓ２４０７は確認応答記録手続き、Ｓ２４０８は受信装置への確認応答受信済みメッセージ送出手続きをそれぞれ表す。
【図２５】実施例３のメッセージ受信手続きのフローチャートである。Ｓ２５０１はリリース時刻判定手続き、Ｓ２５０２は受信メッセージの有無判定手続き、Ｓ２５０３は受信メッセージの重複判定手続き、Ｓ２５０４はリリース予定リストへの追加手続き、Ｓ２５０５はメッセージの復号化手続き、Ｓ２５０６は受信メッセージ廃棄手続き、Ｓ２５０７はメッセージリリース手続き、Ａ２５０８は確認応答送出手続き、Ｓ２５０９は確認応答受信済みメッセージの判定手続き、Ｓ２５１０はタイムアウト判定手続き、をそれぞれ表す。
【図２６】実施例３のメッセージシーケンスである。２６０１は送信装置、２６０２は受信装置をそれぞれ表す。
【図２７】メッセージ配送方式と所要パケット数との関係を示した図である。
【図２８】定数の定義をまとめた図である。
【符号の説明】
１…同報送信装置、　２…受信装置識別子テーブル、　１１－１～ｎ…同報受信クライアント（クライアント装置）、　１２－１～ｎ…同報受信プロトコル装置（受信プロトコル装置）、　１３－１～ｎ…網側インタフェース装置（網インタフェース装置）、　１４－１ｎ…上位インタフェース点、　１５－１～ｎ…下位インタフェース点、　１６－１～ｎ…網側インタフェース点、　１７－１～ｎ…受信装置プロトコル装置識別子、　３１…通信網。

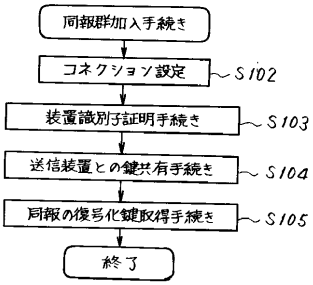
【図１】


クライアント装置
受信プロトコル装置
受信装置識別子
網インタフェース装置
11-n
12-n
13-n
17-n
11-1
12-1
17-1
13-1
上位インタフェース点 14-1
下位インタフェース点 15-1
網側インタフェース点 16-1
通信網
31
同報送信装置
受信装置識別子テーブル
1
2
32-1
32-n
33

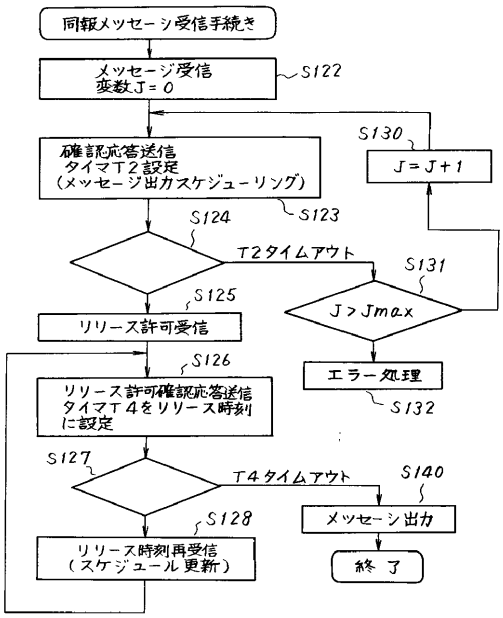
【図２】


同報通信手続き
同報群加入手続き
S101
同報メッセージ受信手続き
S111
S131
鍵変更処理
正常受信
S121
鍵変更
S141
受信エラー処理
S151
同報群通信終了処理
終了

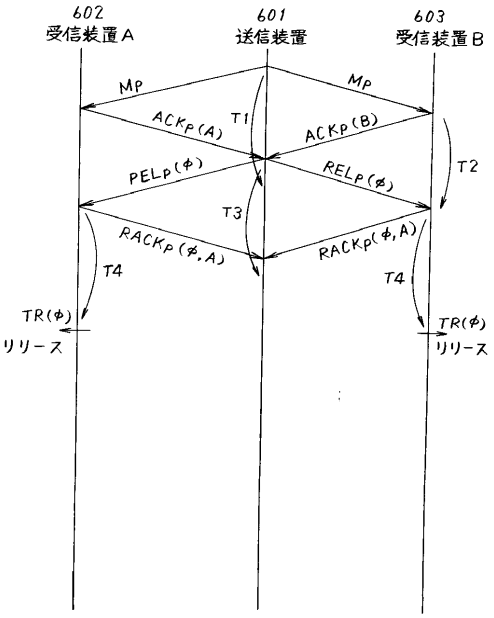
【図３】


同報群加入手続き
コネクション設定
S102
装置識別子証明手続き
S103
送信装置との鍵共有手続き
S104
同報の復号化鍵取得手続き
S105
終了

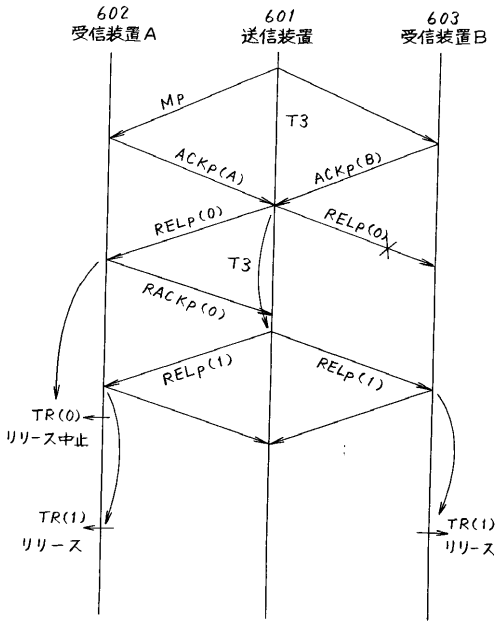
【図４】


同報メッセージ受信手続き
メッセージ受信
変数J=0
S122
確認応答送信
タイマT2設定
(メッセージ出力スケジューリング)
S123
S130
J=J+1
S124
T2タイムアウト
S131
J>Jmax
S125
リリース許可受信
エラー処理
S132
S126
リリース許可確認応答送信
タイマT4をリリース時刻
に設定
S127
T4タイムアウト
S140
メッセージ出力
S128
リリース時刻再受信
(スケジュール更新)
終了

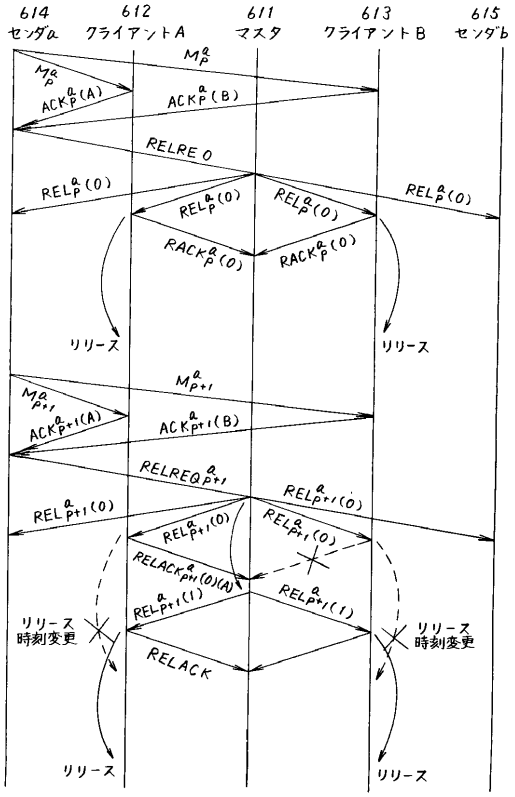
【図５】


602
受信装置A
601
送信装置
603
受信装置B
MP
MP
ACKp(A)
T1
ACKp(B)
T2
PELp(φ)
RELp(φ)
T3
RACKp(φ,A)
RACKp(φ,A)
T4
T4
TR(φ)
リリース
TR(φ)
リリース

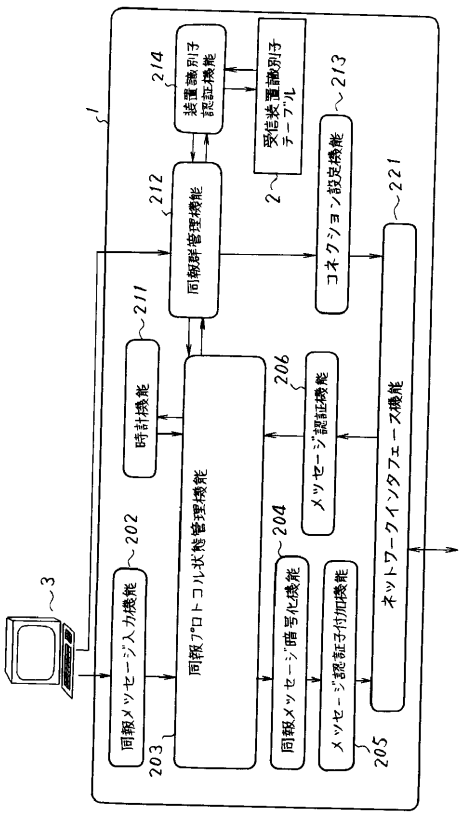
【図６】


602
受信装置A
601
送信装置
603
受信装置B
MP
T3
ACKP(A)
ACKP(B)
RELP(0)
RELP(0)
T3
RACKP(0)
RELP(1)
RELP(1)
TR(0)
リリース中止
TR(1)
リリース
TR(1)
リリース

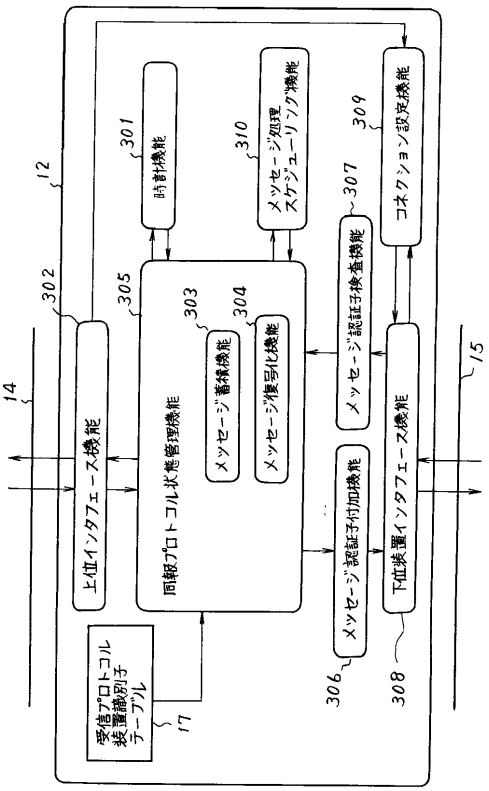
【図７】


614
センダα
612
クライアントA
611
マスタ
613
クライアントB
615
センダb
RELRE 0
リリース
リリース
リリース
リリース
リリース
時刻変更
リリース
時刻変更
RELACK

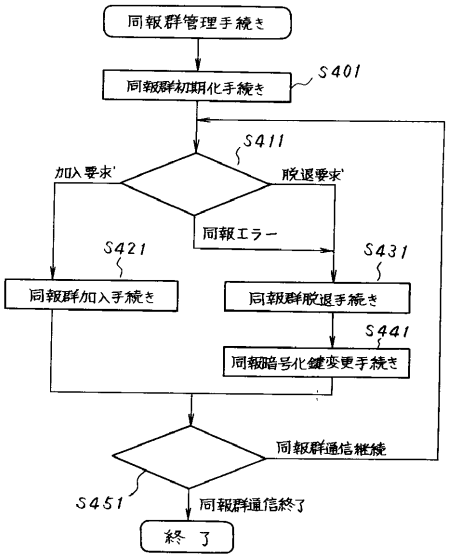
【図８】


同報メッセージ入力機能
同報プロトコル状態管理機能
同報メッセージ暗号化機能
メッセージ認証子付加機能
ネットワークインタフェース機能
時計機能
同報制御管理機能
装置識別子認証機能
受信装置識別子テーブル
コネクション設定機能
メッセージ認証機能

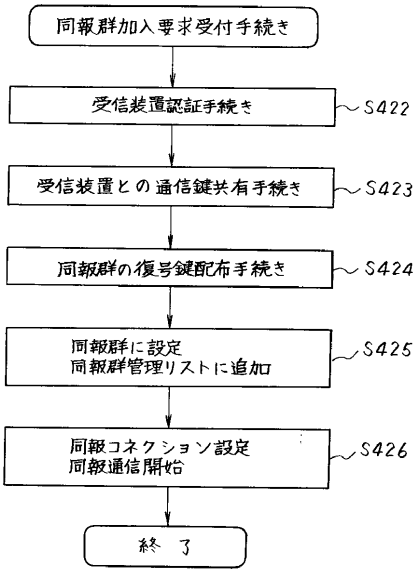
【図９】


上位インタフェース機能
同報プロトコル状態管理機能
メッセージ蓄積機能
メッセージ復号化機能
時計機能
メッセージ処理スケジューリング機能
メッセージ認証子検査機能
コネクション設定機能
メッセージ認証子付加機能
下位装置インタフェース機能
受信プロトコル装置識別子テーブル

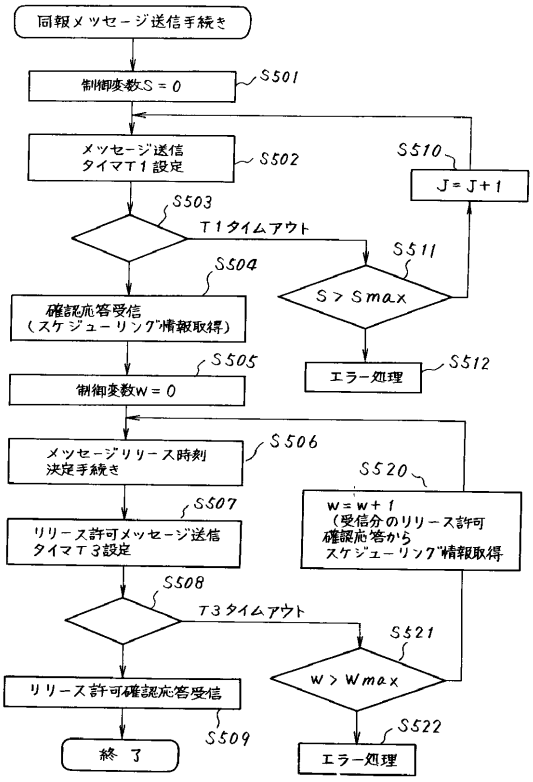
【図１０】



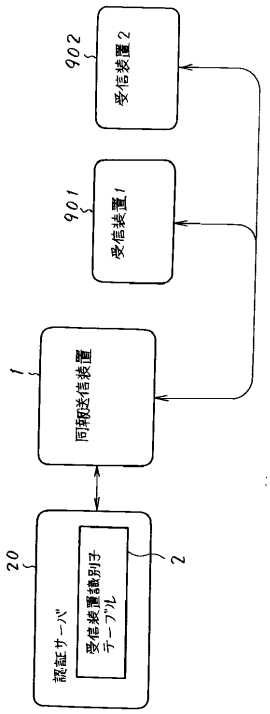
【図１１】



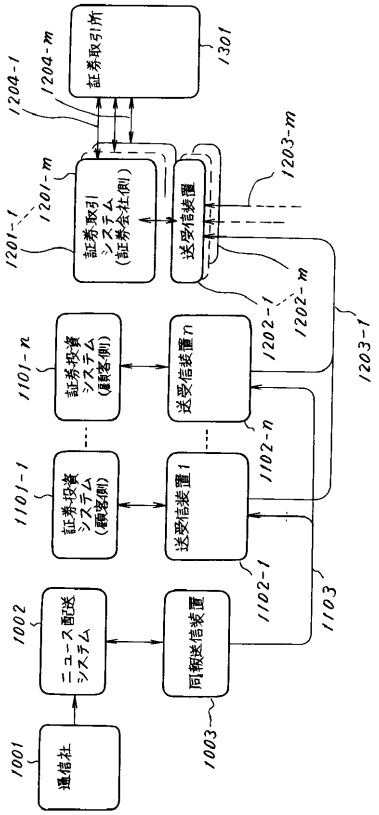
【図１２】



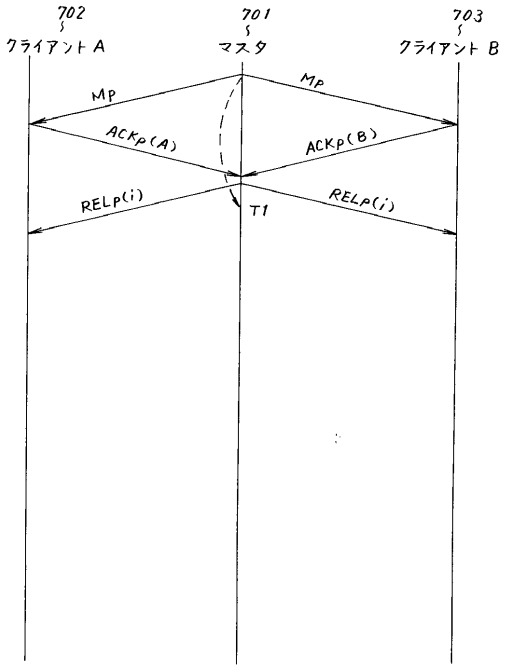
【図１３】



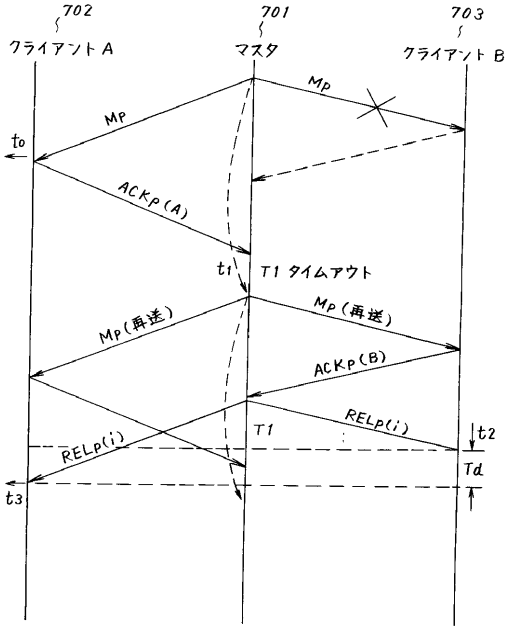
【図１４】



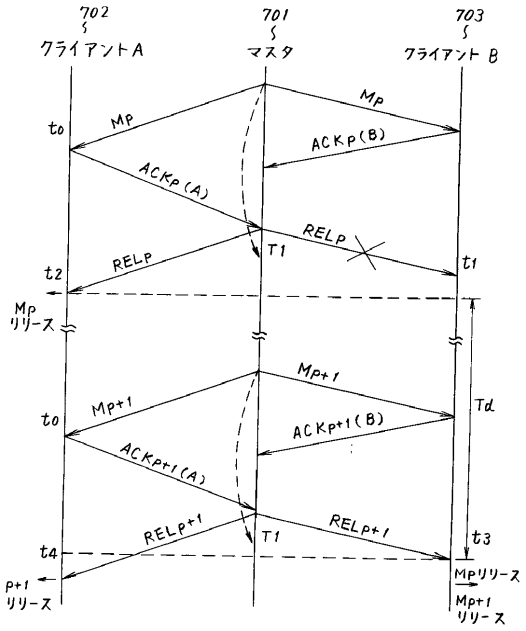
【図１５】



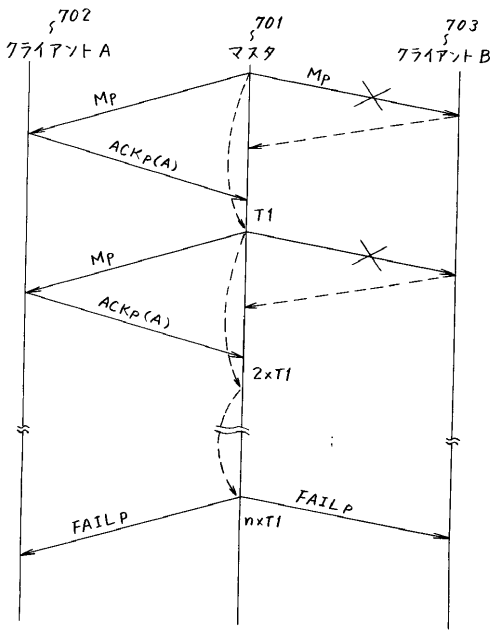
【図１６】



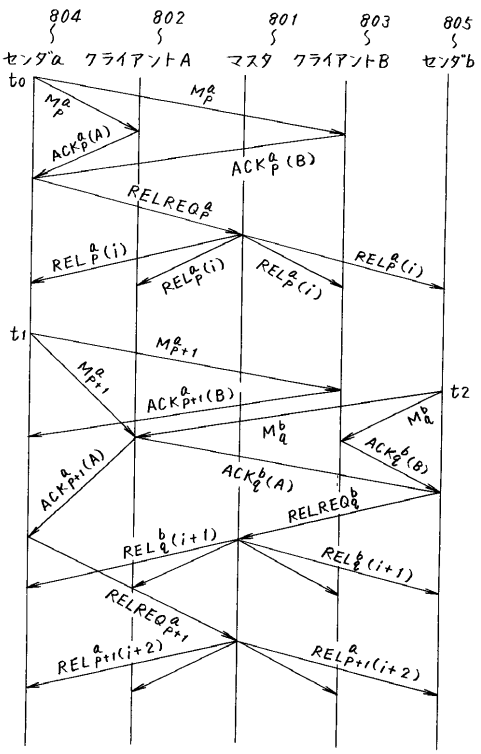
【図１７】



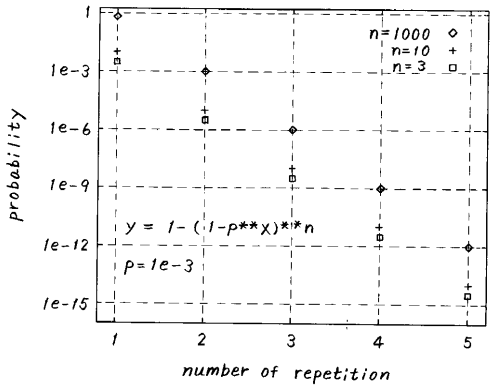
【図１８】



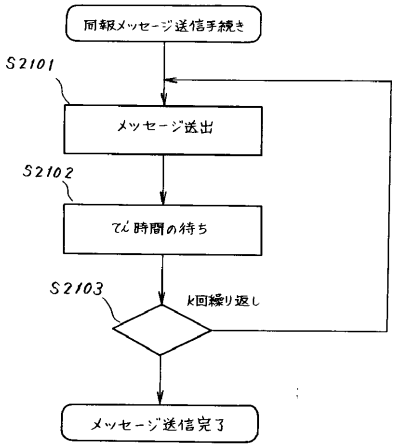
【図１９】



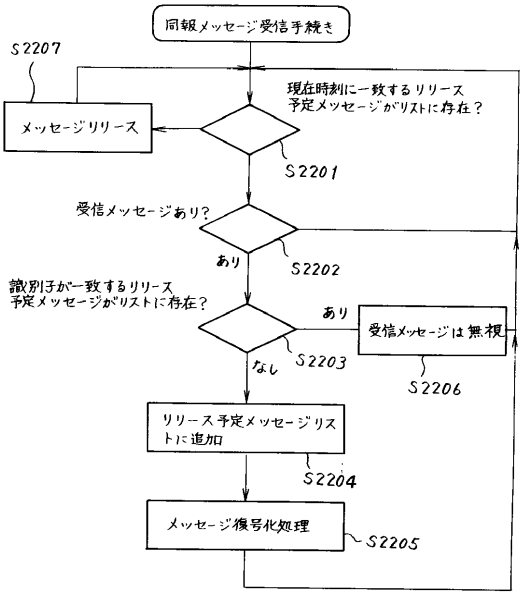
【図２０】



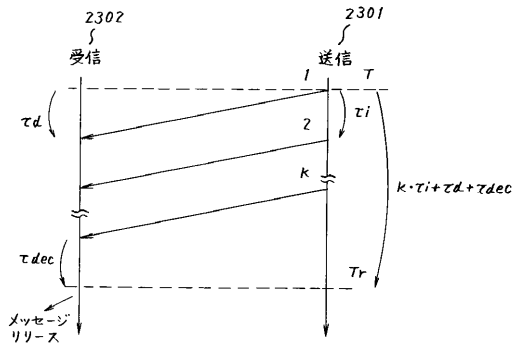
【図２１】



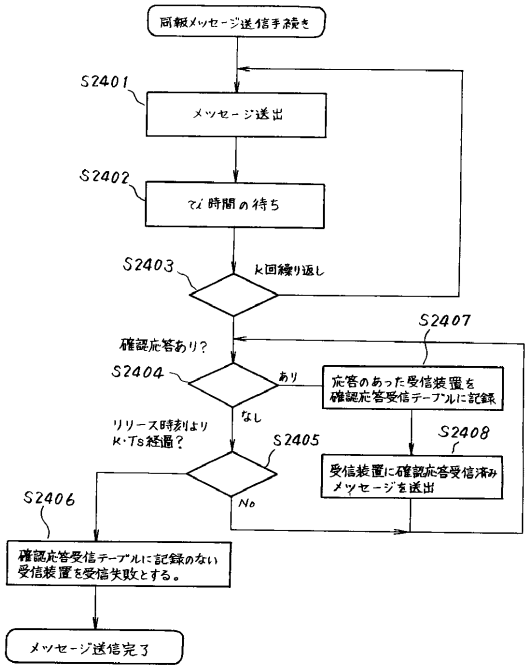
【図２２】



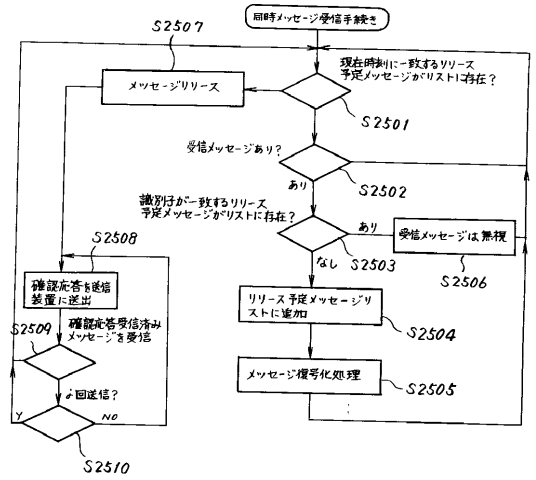
【図２３】



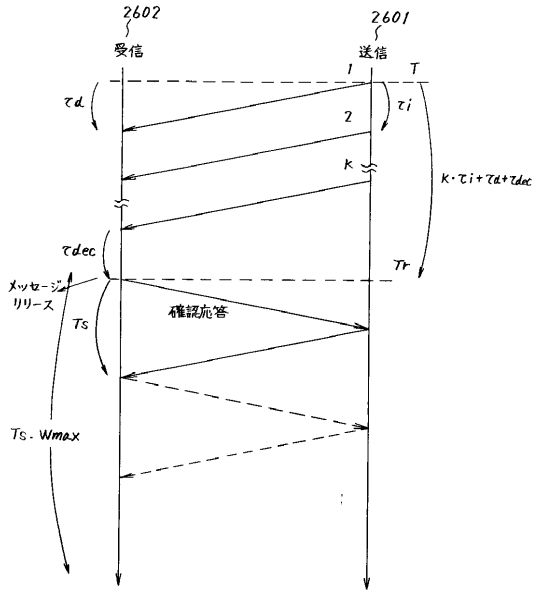
【図２４】



【図２５】



【図２６】



【図２７】

	メッセージ配送に確認あり(2phase)	メッセージ配送に確認なし(1)
リリース時刻の確認応答あり	2m＋2（実施例1）	2m
リリース結果の確認あり	2m＋k＋2（実施例3）	km＋2
リリース結果の確認なし	2m＋k	km（実施例2）

【図２８】

装置 ij 間のメッセージ紛失確率（パラメータ T_d）	$P(t_{ij} > T_d)$
同報群のメッセージ紛失確率（パラメータ T_d）	$P_{loss}(T_d) = max\{P_{loss}(t_{ij} > T_d)\}$
装置 ij 間の応答時間	$RTT_{ij} = t_{ij} + T_P + t_{ji}$
装置 ij 間のタイムアウト時間 T_S（パラメータ P_{tout}）	$P_{tout} > P(RTT_{ij} > T_S)$
パケット送出間隔 T_i（パラメータ P_{loss}）	$P_{Burst}(T_i) \ll P_{loss}$
リリース処理時間	T_{dec}

フロントページの続き

(56)参考文献 特開昭６１－１１４６３３（ＪＰ，Ａ）
特開平５－３４４３０７（ＪＰ，Ａ）
特開平５－２１９０５６（ＪＰ，Ａ）
特開平８－３２５９６（ＪＰ，Ａ）
特開平６－２８９７８１（ＪＰ，Ａ）
特開平４－４７８３２（ＪＰ，Ａ）
特開平６－２９１７６４（ＪＰ，Ａ）
特開平３－２３７８３７（ＪＰ，Ａ）
特開平２－２３４５６０（ＪＰ，Ａ）
特開平８－２９３８２７（ＪＰ，Ａ）
特開平１１－２９６５７９（ＪＰ，Ａ）
電子情報通信学会技術研究報告ＩＳＥＣ９４－２２
情報処理，第３７巻，第２号，第１５５－１６１頁
１９９６年電子情報通信学会通信ソサイエティ大会Ｂ－７８６
THE TRANSACTIONS OF THE IEICE, Vol.E73, No.7, pp.1133-1146

(58)調査した分野(Int.Cl.[7]，ＤＢ名)

H04L 12/18
H04L 12/58
G06F 13/00
H04N 7/173
H04N 1/00
H04N 1/32