(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3910611号
(P3910611)
(45)発行日　平成19年4月25日(2007.4.25)　(24)登録日　平成19年2月2日(2007.2.2)

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

請求項の数 7　(全 25 頁)

(21)出願番号　特願2004-379775(P2004-379775)
(22)出願日　平成16年12月28日(2004.12.28)
(65)公開番号　特開2006-186807(P2006-186807A)
(43)公開日　平成18年7月13日(2006.7.13)
審査請求日　平成18年8月9日(2006.8.9)

早期審査対象出願

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

最終頁に続く

(54)【発明の名称】通信支援サーバ、通信支援方法、および通信支援システム

(57)【特許請求の範囲】
【請求項１】
サーバ装置と、第一の情報処理装置と、第二の情報処理装置と、第三の情報処理装置とを有し、前記第一の情報処理装置が、前記サーバ装置を介さずに、前記第二または前記第三の情報処理装置と行う通信を、前記サーバ装置が支援する通信システムであって、
前記サーバ装置内の鍵共有部が、前記第一の情報処理装置と第一の認証処理を行い、当該第一の認証処理に成功した場合に、当該第一の認証処理の成功に基づいて、前記第一の情報処理装置との暗号通信に用いる第一のサーバ－端末間用鍵を生成して、当該第一のサーバ－端末間用鍵を、前記第一の情報処理装置へ送信すると共に、前記サーバ装置内の暗号鍵格納部に格納し、
前記サーバ装置内の鍵共有部が、前記第二の情報処理装置と第二の認証処理を行い、当該第二の認証処理に成功した場合に、当該第二の認証処理の成功に基づいて、前記第二の情報処理装置との暗号通信に用いる第二のサーバ－端末間用鍵を生成して、当該第二のサーバ－端末間用鍵を、前記第二の情報処理装置へ送信すると共に、前記サーバ装置内の暗号鍵格納部に格納し、
前記サーバ装置内の鍵共有部が、前記第三の情報処理装置と第三の認証処理を行い、当該第三の認証処理に成功した場合に、当該第三の認証処理の成功に基づいて、前記第三の情報処理装置との暗号通信に用いる第三のサーバ－端末間用鍵を生成して、当該第三のサーバ－端末間用鍵を、前記第三の情報処理装置へ送信すると共に、前記サーバ装置内の暗号鍵格納部に格納し、

通信元となる前記第一の情報処理装置の鍵共有部が、前記サーバ装置から受信した、前記第一の認証処理の成功に基づいて生成された、前記第一のサーバー端末間用鍵を、当該第一の情報処理装置内の暗号鍵格納部に格納し、
前記第一の情報処理装置内の通信開始要求部が、通信相手となる前記第二の情報処理装置との通信を前記サーバ装置に要求する際に、当該第一の情報処理装置内の暗号鍵格納部に格納されている第一のサーバー端末間用鍵が使用可能であれば、前記第一の情報処理装置内の暗号通信部が、当該第一のサーバー端末間用鍵を用いて、当該第一の情報処理装置から前記第二の情報処理装置への通信開始要求を暗号化し、
前記第一の情報処理装置内の暗号通信部が、暗号化した前記第二の情報処理装置への通信開始要求を、第一の通信データとして前記サーバ装置へ送信し、
前記サーバ装置内の暗号通信部が、前記第一の通信データを受信し、
前記サーバ装置内の暗号鍵格納部に格納されている前記第一の認証処理の成功に基づく前記第一のサーバー端末間用鍵が使用可能であれば、前記サーバ装置内の暗号通信部が、当該第一のサーバー端末間用鍵を用いて、前記受信した第一の通信データを復号し、
前記第一の通信データを復号した結果が前記第一の情報処理装置から前記第二の情報処理装置への通信開始要求であり、かつ、前記サーバ装置内の暗号鍵格納部に格納されている前記第二のサーバー端末間用鍵が使用可能であれば、前記サーバ装置内の暗号通信部が、当該通信開始要求に基づく第一の接続処理を実行し、
前記第一の情報処理装置内の通信開始要求部が、前記第二の情報処理装置とは異なる前記第三の情報処理装置との通信を前記サーバ装置に要求する際に、前記第二の情報処理装置との通信を前記サーバ装置に要求する前に前記サーバ装置から受信し、前記第一の情報処理装置内の暗号鍵格納部に格納された、前記第一のサーバー端末間用鍵が使用可能であれば、前記第一の情報処理装置内の暗号通信部が、当該第一のサーバー端末間用鍵を用いて、当該第一の情報処理装置から前記第三の情報処理装置への通信開始要求を暗号化し、
前記第一の情報処理装置内の暗号通信部が、暗号化した前記第三の情報処理装置への通信開始要求を、第二の通信データとして前記サーバ装置へ送信し、
前記サーバ装置内の暗号通信部が、前記第二の通信データを受信し、
前記サーバ装置内の暗号鍵格納部に格納されている、前記第一の情報処理装置から前記第一の通信データを受信する前に行った前記第一の認証処理の成功に基づく前記第一のサーバー端末間用鍵が使用可能であれば、前記サーバ装置内の暗号通信部が、当該第一のサーバー端末間用鍵を用いて、前記第二の通信データを復号し、
前記第二の通信データを復号した結果が前記第一の情報処理装置から前記第三の情報処理装置への通信開始要求であり、かつ、前記サーバ装置内の暗号鍵格納部に格納されている前記第三のサーバー端末間用鍵が使用可能であれば、前記サーバ装置内の暗号通信部が、当該通信開始要求に基づく第二の接続処理を実行する
ことを特徴とする通信システム。

【請求項２】
請求項１に記載の通信システムであって、
前記サーバ装置内の暗号通信部は、前記第一の接続処理において、
前記第一の情報処理装置から前記第二の情報処理装置への通信開始要求を、前記サーバ装置内の暗号鍵格納部に格納されている前記第二のサーバー端末間用鍵を用いて暗号化し、
暗号化した前記第二の情報処理装置への通信開始要求を、第三の通信データとして、前記第二の情報処理装置へ送信し、
前記第二の情報処理装置内の暗号通信部は、
前記第三の通信データを受信し、
前記サーバ装置から受信して前記第二の情報処理装置内の暗号鍵格納部に格納された、前記第二の認証処理の成功に基づいて生成された、前記第二のサーバー端末間用鍵が使用可能であれば、受信した第三の通信データを、当該第二のサーバー端末間用鍵を用いて復号し、

復号した第三の通信データが前記第一の情報処理装置から当該第二の情報処理装置への通信開始要求であるならば、前記第二の情報処理装置内の通信データ処理部によって生成された、当該通信開始要求に対して通信を許可するか否かを示す、当該第二の情報処理装置から前記第一の情報処理装置への通信開始応答を、前記第二の情報処理装置内の暗号鍵格納部に格納されている前記第二のサーバー端末間用鍵を用いて暗号化し、

暗号化した前記第一の情報処理装置への通信開始応答を、第四の通信データとして前記サーバ装置へ送信し、

前記サーバ装置内の暗号通信部は、前記第一の接続処理において、

前記第四の通信データを受信し、

受信した第四の通信データを、前記サーバ装置内の暗号鍵格納部に格納されている前記第二のサーバー端末間用鍵を用いて復号し、

復号した第四の通信データが前記第二の情報処理装置から前記第一の情報処理装置への通信開始応答であるならば、当該通信開始応答を、前記サーバ装置内の暗号鍵格納部に格納されている前記第一のサーバー端末間用鍵を用いて暗号化し、

暗号化した前記第二の情報処理装置から前記第一の情報処理装置への通信開始応答を、第五の通信データとして前記第一の情報処理装置へ送信し、

前記第一の情報処理装置内の暗号通信部は、

前記第五の通信データを受信し、

前記暗号鍵格納部に格納されている前記第一のサーバー端末間用鍵を用いて、受信した前記第五の通信データを復号して、前記第二の情報処理装置から当該第一の情報処理装置への通信開始応答を取得し、

前記サーバ装置内の暗号通信部は、前記第二の接続処理において、

前記第一の情報処理装置から前記第三の情報処理装置への通信開始要求を、前記サーバ装置内の暗号鍵格納部に格納されている前記第三のサーバー端末間用鍵を用いて暗号化し、

暗号化した前記第三の情報処理装置への通信開始要求を、第六の通信データとして、前記第三の情報処理装置へ送信し、

前記第三の情報処理装置内の暗号通信部は、

前記第六の通信データを受信し、

前記サーバ装置から受信して前記第三の情報処理装置内の暗号鍵格納部に格納された、前記第三の認証処理の成功に基づいて生成された、前記第三のサーバー端末間用鍵が使用可能であれば、受信した第六の通信データを、当該第三のサーバー端末間用鍵を用いて復号し、

復号した第六の通信データが前記第一の情報処理装置から当該第三の情報処理装置への通信開始要求であるならば、前記第三の情報処理装置内の通信データ処理部によって生成された、当該通信開始要求に対して通信を許可するか否かを示す、当該第三の情報処理装置から前記第一の情報処理装置への通信開始応答を、前記第三の情報処理装置内の暗号鍵格納部に格納されている前記第三のサーバー端末間用鍵を用いて暗号化し、

暗号化した前記第一の情報処理装置への通信開始応答を、第七の通信データとして前記サーバ装置へ送信し、

前記サーバ装置内の暗号通信部は、前記第二の接続処理において、

前記第七の通信データを受信し、

受信した第七の通信データを、前記サーバ装置内の暗号鍵格納部に格納されている前記第三のサーバー端末間用鍵を用いて復号し、

復号した第七の通信データが前記第三の情報処理装置から前記第一の情報処理装置への通信開始応答であるならば、当該通信開始応答を、前記サーバ装置内の暗号鍵格納部に格納されている前記第一のサーバー端末間用鍵を用いて暗号化し、

暗号化した前記第三の情報処理装置から前記第一の情報処理装置への通信開始応答を、第八の通信データとして前記第一の情報処理装置へ送信し、

前記第一の情報処理装置内の暗号通信部は、

前記第八の通信データを受信し、
前記暗号鍵格納部に格納されている前記第一のサーバ－端末間用鍵を用いて、受信した前記第八の通信データを復号して、前記第三の情報処理装置から当該第一の情報処理装置への通信開始応答を取得すること
を特徴とする通信システム。
【請求項３】
請求項１または２に記載の通信システムであって、
各々の前記サーバ－端末間用鍵には、有効期限が対応付けられており、
前記第一の情報処理装置、前記第二の情報処理装置、前記第三の情報処理装置、および前記サーバ装置内の暗号通信部は、
自装置内の暗号鍵格納部に前記サーバ－端末間用鍵が格納されており、かつ、当該サーバ－端末間用鍵に対応付けられている有効期限の経過前であれば、当該サーバ－端末間用鍵が使用可能である、と判断することを特徴とする通信システム。
【請求項４】
請求項３に記載の通信システムにおいて、
前記第一、前記第二、もしくは、前記第三の情報処理装置、または、前記サーバ装置の鍵共有部は、　自装置の前記暗号鍵格納部に格納されている前記サーバ－端末間用鍵に対応づけられている有効期限を経過している場合は、新たな認証処理を行い、当該認証処理に成功した場合に、前記サーバ装置は，当該認証処理を行った情報処理装置との暗号通信に用いる新たなサーバ－端末間用鍵を生成し、生成した前記新たなサーバ－端末間用鍵を、前記認証を行った情報処理装置へ送信すると共に、当該サーバ装置内の暗号鍵格納部へ格納し、
前記新たなサーバ－端末間用鍵を受信した前記情報処理装置の鍵共有部は、当該新たなサーバ－端末間用鍵を、自情報処理装置内の暗号鍵格納部に格納する
ことを特徴とする通信システム。
【請求項５】
請求項４に記載の通信システムにおいて、
前記第一、前記第二、もしくは、前記第三の情報処理装置、または、前記サーバ装置の鍵共有部は、さらに、
自装置の前記暗号鍵格納部に前記サーバ－端末間用鍵が格納されていない場合は、新たな認証処理を行い、当該認証処理に成功した場合に、前記サーバ装置は，当該認証処理を行った情報処理装置との暗号通信に用いる新たなサーバ－端末間用鍵を生成し、生成した前記新たなサーバ－端末間用鍵を、前記認証を行った情報処理装置へ送信すると共に、当該サーバ装置内の暗号鍵格納部へ格納し、
前記新たなサーバ－端末間用鍵を受信した前記情報処理装置の鍵共有部は、当該新たなサーバ－端末間用鍵を、自情報処理装置内の暗号鍵格納部に格納する
ことを特徴とする通信システム。
【請求項６】
請求項２に記載の通信システムであって、
前記第三の通信データは、前記第一の情報処理装置と前記第二の情報処理装置との暗号通信に用いられる第一の端末－端末間用鍵を更に含んで暗号化されたものであり、
前記第二の情報処理装置から前記第一の情報処理装置への通信開始応答が通信許可を示すならば、前記第五の通信データは、前記第一の端末－端末間用鍵を更に含んで暗号化されたものであり、
前記第六の通信データは、前記第一の情報処理装置と前記第三の情報処理装置との暗号通信に用いられる第二の端末－端末間用鍵を更に含んで暗号化されたものであり、
前記第三の情報処理装置から前記第一の情報処理装置への通信開始応答が通信許可を示すならば、前記第八の通信データは、前記第二の端末－端末間用鍵を更に含んで暗号化されたものであり、
前記第一の情報処理装置内の前記暗号通信部は、前記第五の通信データを復号した際に

前記第一の端末－端末間用鍵が含まれていれば，当該第一の端末－端末間用鍵を取得して当該第一の情報処理装置内の暗号鍵格納部に格納し、前記第八の通信データを復号した際に前記第二の端末－端末間用鍵が含まれていれば，当該第二の端末－端末間用鍵を取得して当該第一の情報処理装置内の前記暗号鍵格納部に格納し、
前記第二の情報処理装置内の前記暗号通信部は、前記第三の通信データを復号した際に前記第一の端末－端末間用鍵を取得して当該第二の情報処理装置内の暗号鍵格納部に格納し、
前記第三の情報処理装置内の前記暗号通信部は、前記第六の通信データを復号した際に前記第二の端末－端末間用鍵を取得して当該第三の情報処理装置内の暗号鍵格納部に格納し、
前記第一の情報処理装置内の前記暗号通信部と前記第二の情報処理装置内の前記暗号通信部は、前記第一の端末－端末間用鍵を用いて暗号通信を行い、
前記第一の情報処理装置内の前記暗号通信部と前記第三の情報処理装置内の前記暗号通信部は、前記第二の端末－端末間用鍵を用いて暗号通信を行うこと
を特徴とする通信システム。

【請求項７】
請求項６に記載の通信システムであって、
前記第一の端末－端末間用鍵は、前記第一の接続処理において、前記サーバ装置の鍵情報生成部が作成するものであり、
前記第二の端末－端末間用鍵は、前記第二の接続処理において、前記鍵情報生成部が作成するものであること
を特徴とする通信システム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、インターネット等の通信網を介して暗号通信を行う技術に関する。
【背景技術】
【０００２】
ネットワークを通じて通信端末どうしが暗号通信を行う場合、以下の手順で当該暗号通信のための共通鍵を予め共有し、共有した共通鍵を用いて暗号通信を行う場合がある。通信を開始する通信端末は、通信相手の通信端末の公開鍵を取得する。そして、通信を開始する通信端末は、通信相手の通信端末との暗号通信に用いる共通鍵を生成し、通信相手の通信端末の公開鍵を用いて当該共通鍵を暗号化し、通信相手の通信端末へ送信する。通信相手の通信端末は、自身の公開鍵で暗号化された共通鍵を、通信を開始する通信端末から受信し、自身の公開鍵に対応する秘密鍵で復号することにより、通信を開始する通信端末との暗号通信に用いる共通鍵を共有する。
【０００３】
上記の方法では、通信を開始する通信端末が、複数の通信相手の通信端末のそれぞれと暗号通信を行う場合には、暗号通信のための共通鍵をそれぞれの通信相手の通信端末と共有する必要があり、通信を開始する通信端末の処理負荷が大きくなる場合があった。そこで、暗号通信用の共通鍵を、通信を開始する通信端末と通信相手の通信端末とに配付するサーバをネットワーク上に設け、通信を開始する通信端末と通信相手の通信端末とは、当該サーバから配付された共通鍵を用いて、暗号通信を行う技術が知られている（例えば、非特許文献１参照）。当該非特許文献１に記載の技術では、サーバが、通信を開始する通信端末と通信相手の通信端末との間の暗号通信用の共通鍵を生成し、通信を開始する通信端末と通信相手の通信端末とに配付することにより、通信を開始する通信端末が共通鍵を生成することによる通信端末の処理負荷を軽減している。
【０００４】
【非特許文献１】Mark Baugher 外３名、"MSEC Group Key Management Architecture <draft-ietf-msec-gkmarch-07.txt> "、[online]、January 30, 2003、IETF(Internet Engin

eering Task Force)、P3－13、[平成１６年４月２日検索]、インターネット＜URL:http://www.ietf.org/internet-drafts/draft-ietf-msec-gkmarch-07.txt＞

【発明の開示】

【発明が解決しようとする課題】

【０００５】

しかし、暗号通信の方式には、複数の種類があり、それぞれの種類の暗号通信においても、複数のバージョンが存在する場合がある。そのため、通信を開始する通信端末および通信相手の通信端末は、サーバから配付された共通鍵に基づく暗号通信をサポートしていない場合がある。これにより、サーバから共通鍵を配布された場合であっても、通信を開始する通信端末と通信相手の通信端末とは暗号通信を開始することができない場合があった。

【０００６】

また、通信端末が通信相手と通信を開始する場合、所定の認証手順に従って通信相手の正当性を確認する必要がある。しかしながら、通信端末が、複数の通信相手と暗号通信を行う場合には、通信相手をそれぞれ認証して、正当性を確認する必要があり、通信端末の処理負荷が大きくなる場合があった。

【０００７】

本発明は上記事情を鑑みてなされたものであり、本発明の目的は、複数種類の暗号通信の方式が存在する場合であっても、通信端末間において、確実に暗号化通信が開始されるようにすることにある。また、本発明の他の目的は、認証手順にかかる通信端末の処理負荷を低減することにある。

【課題を解決するための手段】

【０００８】

上記課題を解決するために、通信支援サーバは、通信端末との間で情報を送受信する場合に、当該通信端末の識別情報に対応付けられて、サーバ－端末間用鍵格納部に格納されているサーバ－端末間用鍵の有効期限の経過前である場合は、当該通信端末の識別情報に対応付けられてサーバ－端末間用鍵格納部に格納されている、当該通信端末との暗号通信に用いる鍵であるサーバ－端末間用鍵を用いて当該通信端末との間で暗号通信を行い、当該通信端末の識別情報に対応付けられてサーバ－端末間用鍵格納部に格納されているサーバ－端末間用鍵の有効期限の経過後である場合、または当該通信端末の識別情報に対応するサーバ－端末間用鍵がサーバ－端末間用鍵格納部に格納されていない場合は、鍵共有部に、当該通信端末との暗号通信に用いるサーバ－端末間用鍵の共有を行わせ、新たに共有したサーバ－端末間用鍵を用いて当該通信端末と暗号通信を行う。

【０００９】

例えば、通信端末間の暗号通信を支援する通信支援サーバであって、通信端末毎に、当該通信端末が実施可能な暗号通信の通信条件を、当該通信端末の識別情報に対応付けて格納する通信条件格納部と、通信端末との間で、当該通信端末との暗号通信に用いる鍵であるサーバ－端末間用鍵の共有を行う鍵共有部と、鍵共有部により通信端末との間で共有したサーバ－端末間用鍵を、対応する有効期限と共に、通信端末の識別情報に対応付けて格納するサーバ－端末間用鍵格納部と、サーバ－端末間鍵格納部に格納されているサーバ－端末間用鍵を用いて、当該サーバ－端末間用鍵に対応付けられてサーバ－端末間用鍵格納部に格納されている識別情報を有する通信端末と暗号通信を行う暗号通信部と、暗号通信部を介して通信端末から受信した通信開始要求に含まれる２つの通信端末の識別情報を用いて通信条件格納部を参照し、当該２つの通信端末に共通する通信条件である共通通信条件を抽出する共通通信条件抽出部と、共通通信条件抽出部が抽出した共通通信条件に従った暗号通信で用いる鍵あるいは当該鍵を算出するための種情報である端末－端末間用鍵情報を生成し、生成した端末－端末間用鍵情報を共通通信条件と共に、暗号通信部を介して２つの通信端末のそれぞれへ送信する端末－端末間用鍵情報生成部とを備え、暗号通信部は、通信端末との間で情報を送受信する場合に、当該通信端末の識別情報に対応付けられてサーバ－端末間用鍵格納部に格納されているサーバ－端末間用鍵の有効期限の経過前で

ある場合は、当該通信端末の識別情報に対応付けられてサーバー端末間用鍵格納部に格納されているサーバー端末間用鍵を用いて当該通信端末との間で暗号通信を行い、当該通信端末の識別情報に対応付けられてサーバー端末間用鍵格納部に格納されているサーバー端末間用鍵の有効期限の経過後である場合、または当該通信端末の識別情報に対応するサーバー端末間用鍵がサーバー端末間用鍵格納部に格納されていない場合は、鍵共有部に、当該通信端末との暗号通信に用いるサーバー端末間用鍵の共有を行わせ、新たに共有したサーバー端末間用鍵を用いて当該通信端末と暗号通信を行うことを特徴とする通信支援サーバを提供する。

【発明の効果】

【００１０】

本発明によれば、通信端末は、自身がサポートしている通信条件に基づいて、通信相手の端末と確実に通信を開始することができる。また、暗号鍵の生成に係わる通信端末の負荷を軽減することができる。さらに、認証手順にかかる通信端末の処理負荷を低減することができる。

【発明を実施するための最良の形態】

【００１１】

以下に、本発明の実施の形態を説明する。

図１は、本発明の一実施形態に係る通信支援システム１０の構成を示す。通信支援システム１０は、通信支援サーバ２０および複数の情報処理装置１４を備える。複数の情報処理装置１４のそれぞれは、例えば汎用コンピュータ、携帯電話、またはＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）電話器等の通信端末や、電子認証サーバまたは電子署名検証サーバ等のサービス提供サーバ等であり、インターネット等の通信網１２に接続され、通信網１２を介して互いに通信する。また、それぞれの情報処理装置１４は、通信網１２を介して、同じく通信網１２に接続されている通信支援サーバ２０と通信する。

【００１２】

ここで、複数の情報処理装置１４の中で、２つの情報処理装置１４が通信網１２を介して互いに通信を行う場合、通信網１２内を流れる通信データが、他の情報処理装置１４に取得され、通信内容が漏洩する場合がある。これを回避するために、当該２つの情報処理装置１４間で互いの通信データを暗号化する場合がある。

【００１３】

また、それぞれの情報処理装置１４は、異なる方式や異なるバージョンの複数の暗号方式をサポートしている場合がある。通信元および通信相手の情報処理装置１４がサポートしている暗号通信方式が異なると、通信元の情報処理装置１４がサポートしている暗号方式によって暗号化された通信データを、通信相手の情報処理装置１４は復号できない場合がある。そのため、適切に暗号通信を行うことができない場合があった。そこで、本発明では、通信支援サーバ２０に複数の情報処理装置１４がサポートしている通信条件を予め登録しておき、情報処理装置１４が通信を開始する場合に、自身および通信相手の情報処理装置１４に共通の通信条件に基づいて、通信支援サーバ２０に暗号化に使用する共通鍵等の暗号鍵を発行させる。これにより、通信元の情報処理装置１４と通信相手の情報処理装置１４とは適切に暗号通信を開始することができる。以下、その詳細について説明する。

【００１４】

図２は、通信支援サーバ２０の構成の一例を示すブロック図である。通信支援サーバ２０は、暗号鍵格納部２００、鍵共有部２０２、通信条件格納部２０４、通信条件受付部２０６、暗号通信部２０８、通信開始要求受信部２１０、通信条件抽出部２１２、鍵配布制御部２１４、および鍵情報生成部２１６を備える。鍵共有部２０２は、それぞれの情報処理装置１４との間で、認証等の予め定められた手順に従い、予め定められた暗号通信方式に基づく暗号鍵であるサーバー端末間用鍵の共有を行う。

【００１５】

暗号鍵格納部２００は、鍵共有部２０２が情報処理装置１４と共有したそれぞれのサー

バー端末間用鍵を、それぞれのサーバー端末間用鍵の有効期限と共に、それぞれの情報処理装置１４の識別情報に対応付けて格納する。

【００１６】

暗号通信部２０８は、情報処理装置１４から情報処理装置１４の識別情報と共にアクセスされた場合、当該識別情報に基づいて暗号鍵格納部２００を参照し、当該識別情報に対応付けて格納されている、有効期限内のサーバー端末間用鍵がある場合に、当該識別情報に対応するサーバー端末間用鍵を暗号鍵格納部２００から読み出し、当該サーバー端末間用鍵を用いて情報処理装置１４から受信したデータを復号して通信条件受付部２０６、通信開始要求受信部２１０、および鍵配布制御部２１４へ送る。識別情報に対応付けて暗号鍵格納部２００に格納されている、有効期限内のサーバー端末間用鍵がない場合、暗号通信部２０８は、鍵共有部２０２に情報処理装置１４との間でサーバー端末間用鍵の共有処理を行わせる。

【００１７】

また、暗号通信部２０８は、情報処理装置１４へアクセスする場合、情報処理装置１４へのアクセスに先立って、当該識別情報に基づいて暗号鍵格納部２００を参照し、当該識別情報に対応付けて格納されている、有効期限内のサーバー端末間用鍵がある場合に、当該識別情報に対応するサーバー端末間用鍵を暗号鍵格納部２００から読み出し、当該サーバー端末間用鍵を用いて、鍵情報生成部２１６から受け取ったデータを暗号化して、通信網１２を介して情報処理装置１４へ送る。識別情報に対応付けて暗号鍵格納部２００に格納されている、有効期限内のサーバー端末間用鍵がない場合、暗号通信部２０８は、鍵共有部２０２に情報処理装置１４との間でサーバー端末間用鍵の共有処理を行わせる。

【００１８】

このように、有効期限内のサーバー端末間用鍵が暗号鍵格納部２００に格納されている場合に、鍵共有部２０２によるサーバー端末間用鍵の共有処理を省略することにより、サーバー端末間用鍵の共有処理を通信支援サーバ２０へアクセスする度に行う構成に比べて、通信支援サーバ２０とそれぞれの情報処理装置１４との間の通信を迅速に行うことができる。

【００１９】

通信条件格納部２０４は、情報処理装置１４毎に、当該情報処理装置１４が実施可能な暗号通信の通信条件を、当該情報処理装置１４の識別情報に対応付けて格納する。通信条件とは、例えば、サポートしている暗号アルゴリズムの種類、バージョン、鍵の長さ等の情報である。通信条件受付部２０６は、複数の情報処理装置１４のそれぞれから、暗号通信部２０８を介して、それぞれの情報処理装置１４の識別情報と共に、情報処理装置１４のそれぞれの通信条件を受け付け、受け付けた通信条件を、対応する情報処理装置１４の識別情報に対応付けて通信条件格納部２０４に格納させる。

【００２０】

通信開始要求受信部２１０は、暗号通信部２０８を介して情報処理装置１４のそれぞれから通信を行う２つの情報処理装置１４の識別情報を含む通信開始要求を受信した場合に、受信した通信開始要求を鍵配布制御部２１４へ送り、受信した通信開始要求から通信を行う２つの情報処理装置１４の識別情報を抽出し、抽出した情報処理装置１４の識別情報を通信条件抽出部２１２へ送る。通信条件抽出部２１２は、通信開始要求受信部２１０から受け取った２つの情報処理装置１４の識別情報に基づいて通信条件格納部２０４を参照し、当該２つの情報処理装置１４に共通する通信条件である共通通信条件を抽出する。

【００２１】

鍵情報生成部２１６は、通信条件抽出部２１２が抽出した共通通信条件に従った暗号通信で用いる鍵である端末－端末間用鍵および当該端末－端末間用鍵の有効期限を生成し、生成した端末－端末間用鍵および有効期限を、通信条件抽出部２１２が抽出した共通通信条件と共に鍵配布制御部２１４へ送る。また、他の例として、鍵情報生成部２１６は、通信条件抽出部２１２が抽出した共通通信条件に従った暗号通信で用いる鍵を算出するための種情報である端末－端末間用鍵情報および当該端末－端末間用鍵情報の有効期限を生成

し、生成した端末－端末間用鍵情報および有効期限を、通信条件抽出部２１２が抽出した共通通信条件と共に鍵配布制御部２１４へ送ってもよい。

【００２２】

鍵配布制御部２１４は、通信開始要求受信部２１０より受け取った通信開始要求から通信を行う２つの情報処理装置１４の識別情報を抽出し、抽出した情報処理装置１４の識別情報のうち、通信相手の識別情報に対応する情報処理装置１４へ、鍵情報生成部２１６が生成した端末－端末間用鍵および有効期限を、通信開始要求と共に暗号通信部２０８を介して送信する。また、鍵配布制御部２１４は、送信した通信開始要求に応答して情報処理装置１４が返信した通信開始許可を、暗号通信部２０８を介して受信した場合、受信した通信開始許可に含まれる情報処理装置１４の識別情報を参照して、通信開始要求を送信した情報処理装置１４へ、鍵情報生成部２１６が生成した端末－端末間用鍵および有効期限を、通信開始許可と共に暗号通信部２０８を介して送信する。

【００２３】

このように、通信支援サーバ２０は、共通の通信条件に基づいて端末－端末間用鍵を生成し、生成した端末－端末間用鍵を、通信網１２を介して対応する情報処理装置１４へ送信するので、暗号鍵を生成し、生成した暗号鍵をそれぞれの情報処理装置１４へ配布するのみの構成に比べて、サポートしていない通信条件に基づく暗号鍵が配布されることがなくなり、情報処理装置１４は、通信支援サーバ２０から配布された暗号鍵を用いて、他の情報処理装置１４と確実に暗号通信を開始することができる。

【００２４】

図３は、暗号鍵格納部２００に格納されるデータの構造の一例を示す。暗号鍵格納部２００は、対端末間の暗号通信に用いる暗号鍵であるサーバ－端末間用鍵２００２および当該サーバ－端末間用鍵２００２を使用し続けることができる期限である有効期限２００４を、識別情報２０００に対応付けて格納する。

【００２５】

暗号鍵格納部２００を参照することにより、暗号通信部２０８は、アクセスしてきた情報処理装置１４に対応するサーバ－端末間用鍵を用いて、当該情報処理装置１４と暗号通信を行うことができる。また、暗号鍵格納部２００を参照することにより、暗号通信部２０８は、情報処理装置１４からアクセスされた場合、当該情報処理装置１４の識別情報に対応する、有効期限内のサーバ－端末間用鍵がある場合に、当該識別情報に対応するサーバ－端末間用鍵を暗号鍵格納部２００から読み出し、読み出したサーバ－端末間用鍵を用いてアクセスしてきた情報処理装置１４との間で暗号通信を行うことができる。一方、アクセスしてきた情報処理装置１４に対応する、有効期限内のサーバ－端末間用鍵がない場合、暗号通信部２０８は、鍵共有部２０２にアクセスしてきた情報処理装置１４との間でサーバ－端末間用鍵の共有処理を行わせることができる。

【００２６】

なお、他の例として、通信支援サーバ２０は、通信支援サーバ２０が有する時刻を計時する機能を用いて、有効期限を経過したサーバ－端末間用鍵を暗号鍵格納部２００から削除する手段を有してもよい。この場合、暗号通信部２０８は、アクセスしてきた、あるいはアクセスする情報処理装置１４に対応するサーバ－端末間用鍵が暗号鍵格納部２００に格納されているか否かを判定すればよく、サーバ－端末間用鍵の有効期限を検証する必要がなくなり、より高速に情報処理装置１４との暗号通信を開始することができる。

【００２７】

図４は、通信条件格納部２０４に格納されるデータの構造の一例を示す。通信条件格納部２０４は、複数の通信条件２０４２および当該複数の通信条件２０４２のそれぞれに対応する優先度２０４４を、識別情報２０４０に対応付けて格納する。通信条件格納部２０４を参照することにより、通信条件抽出部２１２は、２つの情報処理装置１４に共通の通信条件を抽出することができる。

【００２８】

また、２つの情報処理装置１４に共通の通信条件が複数存在する場合には、通信条件抽

出部２１２は、複数の共通通信条件の中で、例えば通信開始要求を送信した情報処理装置１４の通信条件であって、かつ優先度が最も高い通信条件を共通通信条件として抽出する。これにより、例えば、処理時間の削減よりも暗号化の強度を高めたい場合や、暗号化の強度を多少犠牲にしてでも処理時間を削減したい場合等の通信開始要求を送信した情報処理装置１４の嗜好に応じた端末間の暗号通信を実現することができる。

【００２９】

なお、共通する通信条件が通信条件格納部２０４内に存在しない場合、通信条件抽出部２１２は、例えば、共通通信条件として例えばＮＵＬＬデータを抽出する。通信条件抽出部２１２がＮＵＬＬデータを抽出した場合、鍵情報生成部２１６は、通信条件抽出部２１２が抽出したＮＵＬＬデータを鍵配布制御部２１４へ送る。鍵配布制御部２１４は、鍵情報生成部２１６からＮＵＬＬデータを受け取った場合、共通の通信条件が存在しない旨を、通信開始要求を送信した情報処理装置１４へ、暗号通信部２０８を介して通知する。

【００３０】

図５は、情報処理装置１４の構成の一例を示すブロック図である。情報処理装置１４は、鍵共有部１４０、対サーバ暗号鍵格納部１４２、対サーバ間暗号通信部１４４、通信条件登録部１４６、通信条件格納部１４８、通信開始要求送信部１５０、通信データ処理部１５２、対端末暗号鍵受信部１５４、対端末間暗号通信部１５６、および対端末暗号鍵格納部１５８を備える。

【００３１】

鍵共有部１４０は、通信支援サーバ２０との間で、認証等の予め定められた手順に従い、サーバ－端末間用鍵の共有を行う。対サーバ暗号鍵格納部１４２は、鍵共有部１４０が通信支援サーバ２０と共有したサーバ－端末間用鍵を、当該サーバ－端末間用鍵の有効期限に対応付けて格納する。

【００３２】

対サーバ間暗号通信部１４４は、通信支援サーバ２０からアクセスされた場合、対サーバ暗号鍵格納部１４２を参照し、対サーバ暗号鍵格納部１４２に格納されている、有効期限内のサーバ－端末間用鍵がある場合に、当該サーバ－端末間用鍵を対サーバ暗号鍵格納部１４２から読み出し、当該サーバ－端末間用鍵を用いて通信支援サーバ２０から受信した通信データを復号して対端末暗号鍵受信部１５４へ送る。対サーバ暗号鍵格納部１４２に格納されている、有効期限内のサーバ－端末間用鍵がない場合、対サーバ間暗号通信部１４４は、鍵共有部１４０に通信支援サーバ２０との間でサーバ－端末間用鍵の共有処理を行わせる。

【００３３】

また、対サーバ間暗号通信部１４４は、通信支援サーバ２０へアクセスする場合、通信支援サーバ２０へのアクセスに先立って、対サーバ暗号鍵格納部１４２を参照し、対サーバ暗号鍵格納部１４２に格納されている、有効期限内のサーバ－端末間用鍵がある場合に、当該サーバ－端末間用鍵を対サーバ暗号鍵格納部１４２から読み出し、当該サーバ－端末間用鍵を用いて、通信条件登録部１４６、通信開始要求送信部１５０、および対端末暗号鍵受信部１５４から受け取った通信データを暗号化して、通信網１２を介して通信支援サーバ２０へ送る。対サーバ暗号鍵格納部１４２に格納されている、有効期限内のサーバ－端末間用鍵がない場合、対サーバ間暗号通信部１４４は、鍵共有部１４０に通信支援サーバ２０との間でサーバ－端末間用鍵の共有処理を行わせる。

【００３４】

通信条件格納部１４８は、情報処理装置１４がサポートしている通信条件を格納する。通信条件登録部１４６は、通信条件格納部１４８を参照して、通信条件が変更された場合に、情報処理装置１４がサポートしている通信条件を通信条件格納部１４８から読み出し、対サーバ間暗号通信部１４４を介して通信支援サーバ２０へ送信する。なお、本例において通信条件登録部１４６は、サポートしている通信条件の一部が変更または追加された場合であっても、通信条件格納部１４８に格納されている全ての通信条件を通信支援サーバ２０へ送信する。

【００３５】
通信データ処理部１５２は、通信相手の情報処理装置１４の識別情報および送信すべき通信データを生成すると共に、対端末間暗号通信部１５６を介して受信した通信データを処理する。通信開始要求送信部１５０は、通信データ処理部１５２が生成した通信相手の情報処理装置１４の識別情報を、自身の情報処理装置１４の識別情報と共に、対サーバ間暗号通信部１４４を介して通信支援サーバ２０へ送信する。
【００３６】
対端末暗号鍵受信部１５４は、通信開始要求送信部１５０が送信した通信開始要求に応答して通信支援サーバ２０から送信された通信開始許可を、自身および通信相手の情報処理装置１４に共通の通信条件に基づいて生成された端末－端末間用鍵、共通通信条件、および有効期限と共に受信し、受信した通信開始許可から通信相手の情報処理装置１４の識別情報を抽出し、抽出した識別情報を通信支援サーバ２０から受信した端末－端末間用鍵、共通通信条件、および有効期限と共に対端末暗号鍵格納部１５８へ送る。対端末暗号鍵格納部１５８は、対端末暗号鍵受信部１５４が通信支援サーバ２０から受信した端末－端末間用鍵、共通通信条件、および有効期限を、対端末暗号鍵受信部１５４が通信開始許可から抽出した通信相手の情報処理装置１４の識別情報に対応付けて格納する。
【００３７】
また、対端末暗号鍵受信部１５４は、他の情報処理装置１４から通信支援サーバ２０を介して通信開始要求を受信した場合、当該通信開始要求を通信データ処理部１５２へ通知する。通信データ処理部１５２は、対端末暗号鍵受信部１５４から通信開始要求を受け取った場合、当該通信開始要求を送信した情報処理装置１４との間で暗号通信を行うか否か判断する。当該通信開始要求を送信した情報処理装置１４との間で暗号通信を行う場合には、通信データ処理部１５２は、対端末暗号鍵受信部１５４に、通信開始要求を送信してきた情報処理装置１４宛てに通信開始許可を、対サーバ間暗号通信部１４４を介して返信させる。一方、当該通信開始要求を送信した情報処理装置１４との間で暗号通信を行わない場合には、通信データ処理部１５２は、対端末暗号鍵受信部１５４に、通信開始要求を送信してきた情報処理装置１４宛てに通信開始を許可しない旨を、対サーバ間暗号通信部１４４を介して返信させる。また、対端末暗号鍵受信部１５４は、通信開始要求に応答して他の情報処理装置１４が送信した通信開始を許可しない旨を受信した場合、その旨を通信データ処理部１５２へ通知する。
【００３８】
対端末間暗号通信部１５６は、通信データ処理部１５２が送信すべき通信データを生成した場合、当該通信データおよび通信相手の情報処理装置１４の識別情報を通信データ処理部１５２から受け取る。そして、対端末間暗号通信部１５６は、通信データ処理部１５２から受け取った通信相手の情報処理装置１４の識別情報に基づいて対端末暗号鍵格納部１５８を参照し、当該識別情報に対応付けて格納されている、有効期限内の端末－端末間用鍵がある場合に、当該識別情報に対応する端末－端末間用鍵および共通通信条件を対端末暗号鍵格納部１５８から読み出す。そして、対端末間暗号通信部１５６は、読み出した共通通信条件に格納されている暗号アルゴリズムやバージョン等の情報に従って、読み出した端末－端末間用鍵によって、通信データ処理部１５２から受け取った通信データを暗号化して通信網１２を介して通信相手の情報処理装置１４へ送信する。通信相手の情報処理装置１４の識別情報に対応付けて対端末暗号鍵格納部１５８に格納されている、有効期限内の端末－端末間用鍵がない場合、対端末間暗号通信部１５６は、通信データ処理部１５２に通信支援サーバ２０から端末－端末間用鍵の配布を受ける必要がある旨を通知する。この通知を受け取ると、通信データ処理部１５２は、通信開始要求送信部１５０に通信開始要求を通信支援サーバ２０へ送信させる。
【００３９】
また、対端末間暗号通信部１５６は、通信網１２を介して当該情報処理装置１４から通信データを受信した場合、受信した通信データに含まれる通信相手の情報処理装置１４の識別情報に基づいて対端末暗号鍵格納部１５８を参照し、当該識別情報に対応付けて格納

されている、有効期限内の端末－端末間用鍵がある場合に、当該識別情報に対応する端末－端末間用鍵および共通通信条件を対端末暗号鍵格納部１５８から読み出し、読み出した共通通信条件に従って、対応する端末－端末間用鍵によって、通信データ処理部１５２から受け取った通信データを復号して通信データ処理部１５２へ送る。通信相手の情報処理装置１４の識別情報に対応付けて対端末暗号鍵格納部１５８に格納されている、有効期限内の端末－端末間用鍵がない場合、対端末間暗号通信部１５６は、通信データを送信した情報処理装置１４へ、通信支援サーバ２０から端末－端末間用鍵の配布を受ける必要がある旨を返信する。

【００４０】

一方、通信相手の情報処理装置１４の識別情報に対応付けて対端末暗号鍵格納部１５８に格納されている、有効期限内の端末－端末間用鍵がない場合、対端末間暗号通信部１５６は、通信データ処理部１５２に通信支援サーバ２０から端末－端末間用鍵の配布を受ける必要がある旨を通知する。この通知を受け取ると、通信データ処理部１５２は、通信開始要求送信部１５０に通信開始要求を通信支援サーバ２０へ送信させる。

【００４１】

なお、他の例として、情報処理装置１４は、情報処理装置１４が有する時刻を計時する機能を用いて、有効期限を経過したサーバ－端末間用鍵を対サーバ暗号鍵格納部１４２から削除する手段を有してもよい。この場合、対サーバ間暗号通信部１４４は、通信支援サーバ２０からアクセスされた場合、または通信支援サーバ２０へアクセスする場合に、サーバ－端末間用鍵が対サーバ暗号鍵格納部１４２に格納されているか否かを判定すればよく、サーバ－端末間用鍵の有効期限を検証する必要がなくなり、より高速に通信支援サーバ２０との暗号通信を開始することができる。

【００４２】

図６は、対サーバ暗号鍵格納部１４２に格納されるデータの構造の一例を示す。対サーバ暗号鍵格納部１４２は、対サーバ間の暗号通信に用いる暗号鍵であるサーバ－端末間用鍵１４２２および当該サーバ－端末間用鍵１４２２を使用し続けることができる期限を示す有効期限１４２４を、自身の鍵共有部１４０に対応付けて格納する。対サーバ暗号鍵格納部１４２を参照することにより、対サーバ間暗号通信部１４４は、サーバ－端末間用鍵を用いて通信支援サーバ２０との間で暗号通信を行うことができる。また、通信支援サーバ２０へアクセスする場合または通信支援サーバ２０からアクセスされた場合のいずれかの場合、対サーバ暗号鍵格納部１４２を参照することにより、対サーバ間暗号通信部１４４は、有効期限内のサーバ－端末間用鍵があれば、当該サーバ－端末間用鍵を用いて通信支援サーバ２０との間で暗号通信を行うことができる。一方、有効期限内のサーバ－端末間用鍵がない場合、対サーバ間暗号通信部１４４は、鍵共有部１４０に通信支援サーバ２０との間でサーバ－端末間用鍵の共有処理を行わせることができる。

【００４３】

図７は、通信条件格納部１４８に格納されるデータの構造の一例を示す。通信条件格納部１４８は、優先度１４８２を、自身の情報処理装置１４がサポートする通信条件１４８０に対応付けて格納する。通信条件格納部１４８を参照することにより、通信条件登録部１４６は、優先度が対応付けられた通信条件を通信支援サーバ２０の通信条件格納部２０４に登録することができ、通信条件抽出部２１２に、優先度に基づいて共通の通信条件を抽出させることができる。従って、通信開始要求を送信した情報処理装置１４の嗜好に応じた端末間の暗号通信を実現することができる。

【００４４】

図８は、対端末暗号鍵格納部１５８に格納されるデータの構造の一例を示す。対端末暗号鍵格納部１５８は、通信相手の情報処理装置１４との間の暗号通信に用いる端末－端末間用鍵１５８２、自身および通信相手の情報処理装置１４に共通の通信条件である共通通信条件１５８４、端末－端末間用鍵１５８２および共通通信条件１５８４を使用し続けることができる期限である有効期限１５８６を、通信相手の情報処理装置１４を識別する情報である通信相手識別情報１５８０に対応付けて格納する。対端末暗号鍵格納部１５８を

参照することにより、対端末間暗号通信部１５６は、通信データ処理部１５２が生成した通信データを送信すべき通信相手の情報処理装置１４の識別情報に対応付けて格納されている、有効期限内の端末－端末間用鍵があるか否かを判定することができる。

【００４５】

図９は、通信支援サーバ２０の動作の一例を示すフローチャートである。電源投入等の所定のタイミングで、本フローチャートに示す通信支援サーバ２０の動作が開始する。まず、暗号通信部２０８は、情報処理装置１４からアクセスされたか否かを判定する（Ｓ１００）。情報処理装置１４からアクセスされていない場合（Ｓ１００：Ｎｏ）、暗号通信部２０８は、情報処理装置１４からアクセスされるまでステップ１００を繰り返す。

【００４６】

ステップ１００において、情報処理装置１４からアクセスされた場合（Ｓ１００：Ｙｅｓ）、暗号通信部２０８は、サーバ－端末間用鍵の共有を要求する通信データか否かを判定する（Ｓ１０２）。サーバ－端末間用鍵の共有を要求する通信データである場合（Ｓ１０２：Ｙｅｓ）、暗号通信部２０８は、鍵共有部２０２に、アクセスしてきた情報処理装置１４との間でサーバ－端末間用鍵の共有処理を行わせ（Ｓ１０４）、再びステップ１００に示した処理を行う。

【００４７】

ステップ１０４において、鍵共有部２０２は、例えば、サーバ－端末間の暗号通信に使用する一つ以上のパラメータの候補を情報処理装置１４の鍵共有部１４０から受け付け、受け付けたパラメータの候補の中から、暗号通信部２０８がサポートしているパラメータを一つ選択し、鍵共有部１４０へ返信することにより、鍵共有部２０２は、鍵共有部１４０との間で暗号通信に用いるパラメータを共有する。そして、鍵共有部２０２は、通信支援サーバ２０の公開鍵証明書を鍵共有部１４０へ送信すると共に、情報処理装置１４の公開鍵証明書を鍵共有部１４０に要求する。そして、鍵共有部２０２は、鍵共有部１４０から受信した公開鍵証明書の有効期限、署名を検証することにより、公開鍵証明書を検証する。

【００４８】

公開鍵証明書の検証に成功した場合、鍵共有部２０２と鍵共有部１４０とは、共有したパラメータを電子署名と共に相手へ送信し、受信した電子署名を検証することにより、通信相手を認証する。そして、鍵共有部２０２と鍵共有部１４０とが互いの認証に成功した場合に、鍵共有部１４０は、共有したパラメータに基づいて、通信支援サーバ２０の暗号通信部２０８との暗号通信に用いるサーバ－端末間用鍵を生成し、生成したサーバ－端末間用鍵を通信支援サーバ２０の公開鍵を用いて暗号化して鍵共有部２０２へ送信することにより、鍵共有部２０２との間で暗号通信に用いるサーバ－端末間用鍵を共有する。

【００４９】

なお、鍵共有部２０２は、外部に設けられた検証サーバに、鍵共有部１４０から受信した公開鍵証明書の検証を依頼してもよい。鍵共有部２０２から公開鍵証明書を受信した場合、検証サーバは、当該公開鍵証明書に記載された認証局をたどり、行き着いた認証局から当該公開鍵証明書の失効情報を入手することにより、入手した失効情報を検証することにより、受信した公開鍵証明書を検証する。これにより、鍵共有部２０２は、より厳密に情報処理装置１４の公開鍵証明書を検証することができる。

【００５０】

ステップ１０２において、受信した通信データがサーバ－端末間用鍵の共有を要求する通信データでない場合（Ｓ１０２：Ｎｏ）、暗号通信部２０８は、アクセスしてきた情報処理装置１４の識別情報に基づいて暗号鍵格納部２００を参照し、当該識別情報に対応付けて格納されている、有効期限内のサーバ－端末間用鍵があるか否かを判定する（Ｓ１０６）。有効期限内の、対応するサーバ－端末間用鍵がない場合（Ｓ１０６：Ｎｏ）、暗号通信部２０８は、鍵共有部２０２に、サーバ－端末間用鍵の共有処理を行う必要がある旨を、アクセスしてきた情報処理装置１４へ通知させ（Ｓ１２８）、再びステップ１００に示した処理を行う。

【００５１】
ステップ１０６において、有効期限内の、対応するサーバー端末間用鍵がある場合（Ｓ１０６：Ｙｅｓ）、暗号通信部２０８は、対応するサーバー端末間用鍵を暗号鍵格納部２００から読み出し、読み出したサーバー端末間用鍵を用いて受信した通信データを復号し、復号した通信データを通信条件受付部２０６、通信開始要求受信部２１０、および鍵配布制御部２１４へ送る（Ｓ１０８）。次に、通信条件受付部２０６は、受信した通信データが通信条件の登録を要求するデータか、それ以外かを判定する（Ｓ１１０）。受信した通信データが通信条件の登録を要求するデータである場合（Ｓ１１０：通信条件登録）、通信条件受付部２０６は、受信した通信データに含まれる通信条件を、当該通信データを送信した情報処理装置１４の識別情報に対応付けて通信条件格納部２０４に格納し（Ｓ１１２）、暗号通信部２０８は、再びステップ１００に示した処理を行う。

【００５２】
受信した通信データが通信条件の登録を要求するデータ以外である場合（Ｓ１１０：それ以外）、通信開始要求受信部２１０および鍵配布制御部２１４は、受信した通信データが通信開始要求を示すデータか、通信開始要求に応答して返信された通信開始許可を示すデータかを判定する（Ｓ１１４）。受信した通信データが通信許可を示すデータである場合（Ｓ１１４：通信許可）、鍵配布制御部２１４は、鍵情報生成部２１６が生成した端末－端末間用鍵および当該端末－端末間用鍵の有効期限を、通信開始許可と共に暗号通信部２０８を介して、通信開始要求を送信した情報処理装置１４へ送信し（Ｓ１１６）、暗号通信部２０８は、再びステップ１００に示した処理を行う。

【００５３】
ステップ１１４において、受信した通信データが通信開始要求を示すデータである場合（Ｓ１１４：通信開始要求）、通信開始要求受信部２１０は、受信した通信開始要求から通信を行う２つの情報処理装置１４の識別情報を抽出し、抽出した情報処理装置１４の識別情報を通信条件抽出部２１２へ送る。そして、通信条件抽出部２１２は、通信開始要求受信部２１０から受け取った２つの情報処理装置１４の識別情報に基づいて通信条件格納部２０４を参照し、当該２つの情報処理装置１４に共通する通信条件である共通通信条件を抽出する（Ｓ１１８）。

【００５４】
次に、鍵情報生成部２１６は、通信条件抽出部２１２が抽出した共通通信条件に従った暗号通信で用いる端末－端末間用鍵および当該端末－端末間用鍵の有効期限を生成し、生成した端末－端末間用鍵および有効期限を、通信条件抽出部２１２が抽出した共通通信条件と共に鍵配布制御部２１４へ送る。鍵配布制御部２１４は、通信開始要求受信部２１０より受け取った通信開始要求から通信を行う２つの情報処理装置１４の識別情報を抽出し、抽出した情報処理装置１４の識別情報のうち、通信相手の情報処理装置１４の識別情報を宛先として、鍵情報生成部２１６が生成した端末－端末間用鍵および有効期限、ならびに、通信条件抽出部２１２が抽出した共通通信条件を、通信開始要求と共に暗号通信部２０８へ送る（Ｓ１２０）。

【００５５】
次に、暗号通信部２０８は、鍵配布制御部２１４から宛先として受け取った情報処理装置１４の識別情報に基づいて暗号鍵格納部２００を参照し、当該識別情報に対応付けて格納されている、有効期限内のサーバー端末間用鍵があるか否かを判定する（Ｓ１２２）。有効期限内の、対応するサーバー端末間用鍵がある場合（Ｓ１２２：Ｙｅｓ）、暗号通信部２０８は、対応するサーバー端末間用鍵を暗号鍵格納部２００から読み出し、読み出したサーバー端末間用鍵を用いて、鍵配布制御部２１４から受け取った端末－端末間用鍵および有効期限、ならびに、通信条件抽出部２１２が抽出した共通通信条件を、通信開始要求と共に暗号化して、通信相手の情報処理装置１４へ送信し（Ｓ１２６）、暗号通信部２０８は、再びステップ１００に示した処理を行う。

【００５６】
ステップ１２２において、有効期限内の、対応するサーバー端末間用鍵がない場合（Ｓ

１２２：Ｎｏ）、暗号通信部２０８は、鍵共有部２０２に、通信相手の情報処理装置１４との間でサーバ－端末間用鍵の共有処理を行わせ（Ｓ１２４）、ステップ１２６に示した処理を行う。

【００５７】

図１０は、情報処理装置１４が通信支援サーバ２０または他の情報処理装置１４にアクセスする場合の情報処理装置１４の動作の一例を示すフローチャートである。電源投入等の所定のタイミングで、本フローチャートに示す情報処理装置１４の動作が開始する。まず、通信データ処理部１５２は、送信すべき通信データが発生したか否かを判定する（Ｓ２００）。送信すべき通信データが発生した場合（Ｓ２００：Ｙｅｓ）、対端末間暗号通信部１５６は、当該通信データおよび通信相手の情報処理装置１４の識別情報を通信データ処理部１５２から受け取り、受け取った通信相手の情報処理装置１４の識別情報に基づいて対端末暗号鍵格納部１５８を参照し、当該識別情報に対応付けて格納されている、有効期限内の端末－端末間用鍵があるか否かを判定する（Ｓ２０２）。有効期限内の、対応する端末－端末間用鍵がある場合（Ｓ２０２：Ｙｅｓ）、対端末間暗号通信部１５６は、対応する端末－端末間用鍵を対端末暗号鍵格納部１５８から読み出し、読み出した端末－端末間用鍵用いて通信データ処理部１５２から受け取った通信データを暗号化して通信網１２を介して通信相手の情報処理装置１４へ送信し（Ｓ２０４）、通信データ処理部１５２は、再びステップ２００に示した処理を行う。

【００５８】

ステップ２０２において、有効期限内の、対応する端末－端末間用鍵がない場合（Ｓ２０２：Ｎｏ）、対端末間暗号通信部１５６は、通信支援サーバ２０から端末－端末間用鍵の配布を受ける必要がある旨を通信データ処理部１５２に通知する。この通知を受け取ると、通信データ処理部１５２は、通信開始要求送信部１５０に通信開始要求を、対サーバ間暗号通信部１４４を介して通信支援サーバ２０へ送信させる。この場合、対サーバ間暗号通信部１４４は、対サーバ暗号鍵格納部１４２に格納されている、有効期限内のサーバ－端末間用鍵があるか否かを判定する（Ｓ２０６）。有効期限内のサーバ－端末間用鍵がある場合（Ｓ２０６：Ｙｅｓ）、対サーバ間暗号通信部１４４は、サーバ－端末間用鍵を対サーバ暗号鍵格納部１４２から読み出し、読み出したサーバ－端末間用鍵を用いて、通信開始要求送信部１５０から受け取った通信開始要求を暗号化して、通信網１２を介して通信支援サーバ２０へ送信し（Ｓ２１０）、通信データ処理部１５２は、再びステップ２００に示した処理を行う。

【００５９】

ステップ２０６において、有効期限内のサーバ－端末間用鍵がない場合（Ｓ２０６：Ｎｏ）、対サーバ間暗号通信部１４４は、鍵共有部１４０に、通信支援サーバ２０との間でサーバ－端末間用鍵の共有処理を行わせ（Ｓ２０８）、ステップ２１０に示した処理を行う。

【００６０】

ステップ２００において、送信すべき通信データが発生していない場合（Ｓ２００：Ｎｏ）、通信条件登録部１４６は、通信条件格納部１４８を参照して、通信条件格納部１４８に格納された通信条件が変更されたか否かを判定する（Ｓ２１２）。通信条件が変更されていない場合（Ｓ２１２：Ｎｏ）、通信データ処理部１５２は、再びステップ２００に示した処理を行う。

【００６１】

ステップ２１２において、通信条件が変更された場合（Ｓ２１２：Ｙｅｓ）、通信条件登録部１４６は、通信条件格納部１４８に格納されている通信条件を全て読み出し、読み出した通信条件を含む通信条件登録要求を生成し、生成した通信条件登録要求を対サーバ間暗号通信部１４４へ送る。次に、対サーバ間暗号通信部１４４は、対サーバ暗号鍵格納部１４２に格納されている、有効期限内のサーバ－端末間用鍵があるか否かを判定する（Ｓ２１４）。有効期限内のサーバ－端末間用鍵がある場合（Ｓ２１４：Ｙｅｓ）、対サーバ間暗号通信部１４４は、サーバ－端末間用鍵を対サーバ暗号鍵格納部１４２から読み出

し、読み出したサーバー端末間用鍵を用いて、通信条件登録部１４６から受け取った通信条件登録要求を暗号化して、通信網１２を介して通信支援サーバ２０へ送信し（Ｓ２１８）、通信データ処理部１５２は、再びステップ２００に示した処理を行う。

【００６２】

ステップ２１４において、有効期限内のサーバー端末間用鍵がない場合（Ｓ２１４：Ｎｏ）、対サーバ間暗号通信部１４４は、鍵共有部１４０に、通信支援サーバ２０との間でサーバー端末間用鍵の共有処理を行わせ（Ｓ２１６）、ステップ２１８に示した処理を行う。

【００６３】

図１１は、情報処理装置１４が通信支援サーバ２０または他の情報処理装置１４からアクセスされる場合の情報処理装置１４の動作の一例を示すフローチャートである。電源投入等の所定のタイミングで、本フローチャートに示す情報処理装置１４の動作が開始する。まず、対サーバ間暗号通信部１４４および対端末間暗号通信部１５６は、通信支援サーバ２０または他の情報処理装置１４のいずれかからアクセスされたか否かを判定する（Ｓ３００）。通信支援サーバ２０または他の情報処理装置１４のいずれからもアクセスされない場合（Ｓ３００：Ｎｏ）、対サーバ間暗号通信部１４４および対端末間暗号通信部１５６は、通信支援サーバ２０または他の情報処理装置１４のいずれかからアクセスされるまでステップ３００を繰り返す。

【００６４】

ステップ３００において、通信支援サーバ２０または他の情報処理装置１４のいずれかからアクセスがあった場合（Ｓ３００：Ｙｅｓ）、対サーバ間暗号通信部１４４は、当該アクセスが通信支援サーバ２０からのものであるか否かを判定する（Ｓ３０２）。当該アクセスが通信支援サーバ２０からのものではない、すなわち当該アクセスが他の情報処理装置１４からのものである場合（Ｓ３０２：Ｎｏ）、対端末間暗号通信部１５６は、対端末暗号鍵格納部１５８を参照して、通信網１２を介して通信データと共に他の情報処理装置１４から受信した情報処理装置１４の識別情報に基づいて対端末暗号鍵格納部１５８を参照し、当該識別情報に対応付けて格納されている、有効期限内の端末－端末間用鍵があるか否かを判定する（Ｓ３２４）。有効期限内の、対応する端末－端末間用鍵がある場合（Ｓ３２４：Ｙｅｓ）、対端末間暗号通信部１５６は、対応する端末－端末間用鍵を対端末暗号鍵格納部１５８から読み出し、読み出した端末－端末間用鍵用いて、他の情報処理装置１４から受信した通信データを復号して通信データ処理部１５２へ送ると共に、受信した通信データに応じて通信データ処理部１５２が送信する通信データを暗号化して通信網１２を介して通信相手の情報処理装置１４へ返信し（Ｓ３２６）、対サーバ間暗号通信部１４４および対端末間暗号通信部１５６は、再びステップ３００に示した処理を行う。

【００６５】

ステップ３２４において、有効期限内の、対応する端末－端末間用鍵がない場合（Ｓ３２４：Ｎｏ）、対端末間暗号通信部１５６は、アクセスしてきた他の情報処理装置１４に通信支援サーバ２０から端末－端末間用鍵の配布を受ける必要がある旨を返信し（Ｓ３２８）、対サーバ間暗号通信部１４４および対端末間暗号通信部１５６は、再びステップ３００に示した処理を行う。

【００６６】

ステップ３０２において、通信支援サーバ２０からのアクセスがあった場合（Ｓ３０２：Ｙｅｓ）、対サーバ間暗号通信部１４４は、対サーバ暗号鍵格納部１４２に格納されている、有効期限内のサーバー端末間用鍵があるか否かを判定する（Ｓ３０４）。有効期限内のサーバー端末間用鍵がある場合（Ｓ３０４：Ｙｅｓ）、対サーバ間暗号通信部１４４は、サーバー端末間用鍵を対サーバ暗号鍵格納部１４２から読み出し、読み出したサーバー端末間用鍵を用いて、通信支援サーバ２０から受信したデータを復号する（Ｓ３０８）。有効期限内のサーバー端末間用鍵がない場合（Ｓ３０４：Ｎｏ）、対サーバ間暗号通信部１４４は、鍵共有部１４０に、通信支援サーバ２０との間でサーバー端末間用鍵の共有処理を行わせ（Ｓ３０６）、ステップ３０８に示した処理を行う。

【００６７】
ステップ３０６の処理は、例外的な処理であり、例えば通信支援サーバ２０と情報処理装置１４との内部時計のずれ等によって発生するものである。
【００６８】
次に、対端末暗号鍵受信部１５４は、通信支援サーバ２０から受信した通信データが通信開始要求を示すデータか、通信開始要求に応答して通信支援サーバ２０を介して返信された通信開始許可を示すデータかを判定する（Ｓ３１０）。受信した通信データが通信開始要求である場合（Ｓ３１０：通信開始要求）、対端末暗号鍵受信部１５４は、受信した通信開始要求を通信データ処理部１５２へ送り、通信開始要求と共に受信した端末－端末間用鍵および当該端末－端末間用鍵の有効期限を、通信開始要求を送信した情報処理装置１４の識別情報に対応付けて対端末暗号鍵格納部１５８に格納する（Ｓ３１２）。
【００６９】
次に、通信データ処理部１５２は、通信開始要求を送信してきた情報処理装置１４と通信を行うか否かを判定する（Ｓ３１８）。通信開始要求を送信してきた情報処理装置１４と通信を行う場合（Ｓ３１８：Ｙｅｓ）、通信データ処理部１５２は、通信開始要求送信部１５０に通信開始許可を、対サーバ間暗号通信部１４４を介して通信支援サーバ２０へ送信させ（Ｓ３２２）、対サーバ間暗号通信部１４４および対端末間暗号通信部１５６は、再びステップ３００に示した処理を行う。この場合、対サーバ間暗号通信部１４４は、対サーバ暗号鍵格納部１４２に格納されているサーバ－端末間用鍵を用いて当該通信開始許可を暗号化して通信網１２を介して通信支援サーバ２０へ送信する。
【００７０】
ステップ３１８において、通信開始要求を送信してきた情報処理装置１４と通信を行わない場合（Ｓ３１８：Ｎｏ）、通信データ処理部１５２は、通信開始要求送信部１５０に通信開始を許可しない旨を、対サーバ間暗号通信部１４４を介して通信支援サーバ２０へ送信させ（Ｓ３２０）、対サーバ間暗号通信部１４４および対端末間暗号通信部１５６は、再びステップ３００に示した処理を行う。
【００７１】
ステップ３１０において、受信した通信データが通信開始許可である場合（Ｓ３１０：通信開始許可）、対端末暗号鍵受信部１５４は、受信した通信開始許可を通信データ処理部１５２へ送り、通信開始許可と共に受信した端末－端末間用鍵および当該端末－端末間用鍵の有効期限を、通信開始許可を送信した情報処理装置１４の識別情報に対応付けて対端末暗号鍵格納部１５８に格納する（Ｓ３１４）。そして、対端末間暗号通信部１５６は、通信開始許可と共に受信した端末－端末間用鍵を対端末暗号鍵格納部１５８から読み出し、読み出した端末－端末間用鍵用いて、通信データ処理部１５２が生成した通信データを暗号化して、通信網１２を介して他の情報処理装置１４へ送信すると共に、他の情報処理装置１４から通信網１２を介して受信した通信データを復号して通信データ処理部１５２へ送る（Ｓ３１６）。そして、対サーバ間暗号通信部１４４および対端末間暗号通信部１５６は、再びステップ３００に示した処理を行う。
【００７２】
ここで、図９、図１０、および図１１に示したそれぞれの処理の関係をまとめると次のようになる。
【００７３】
暗号通信を行う情報処理装置１４どうしが、通信相手の情報処理装置１４に対応する有効期限内の端末－端末間用鍵を有する場合、図１０のステップ２０４において、発信側の情報処理装置１４が端末－端末間用鍵を用いて通信データを暗号化して通信相手の情報処理装置１４へ送信する。そして、図１１のステップ３２６において、着信側の情報処理装置１４が受信したデータを端末－端末間用鍵を用いて復号する。その後、２つ情報処理装置１４は、対応する端末－端末間用鍵を用いて暗号通信を行う。
【００７４】
また、有効期限内のサーバ－端末間用鍵を有する情報処理装置１４が、通信支援サーバ

２０へ通信条件を登録する場合、図１０のステップ２１８において、サーバ－端末間用鍵を用いて通信条件を暗号化して通信支援サーバ２０へ送信する。これを受けて、通信支援サーバ２０は、図９のステップ１１２において、受信した通信条件を通信条件格納部２０４に格納する。

【００７５】

また、暗号通信を行う情報処理装置１４どうしが、通信相手の情報処理装置１４に対応する有効期限内の端末－端末間用鍵を有していなく、かつ有効期限内のサーバ－端末間用鍵を有していない場合、図１０のステップ２０８において、発信側の情報処理装置１４は、通信支援サーバ２０との間でサーバ－端末間用鍵の共有処理を行う。このとき、通信支援サーバ２０は、図９のステップ１０４において、アクセスしてきた情報処理装置１４との間でサーバ－端末間用鍵の共有処理を行う。

【００７６】

その後、発信側の情報処理装置１４は、図１０のステップ２１０において、通信支援サーバ２０との間で共有したサーバ－端末間用鍵を用いて、通信開始要求を暗号化して通信支援サーバ２０へ送信する。これを受けて、通信支援サーバ２０は、図９のステップ１１８および１２０において、暗号通信を行う２つの情報処理装置１４の通信条件に基づいて端末－端末間用鍵を生成する。

【００７７】

そして、通信支援サーバ２０は、図９のステップ１２４において、着信側の情報処理装置１４との間でサーバ－端末間用鍵の共有処理を行う。このとき、着信側の情報処理装置１４は、図１１のステップ３０６において、通信支援サーバ２０との間でサーバ－端末間用鍵の共有処理を行う。

【００７８】

そして、通信支援サーバ２０は、図９のステップ１２６において、通信開始要求および端末－端末間用鍵等を、共有したサーバ－端末間用鍵で暗号化して、着信側の情報処理装置１４へ送信する。このとき、着信側の情報処理装置１４は、図１１のステップ３１２において、通信開始要求と共に受信した端末－端末間用鍵等を格納し、ステップ３２２において、通信許可をサーバ－端末間用鍵で暗号化して通信支援サーバ２０へ送信する。これを受けて、通信支援サーバ２０は、図９のステップ１１６において、通信開始許可および端末－端末間用鍵等を、サーバ－端末間用鍵で暗号化して、発信側の情報処理装置１４へ送信する。これを受けて、発信側の情報処理装置１４は、図１１のステップ３１４および３１６において、通信開始許可と共に受信した端末－端末間用鍵等を格納して、格納した端末－端末間用鍵を用いて着信側の報処理装置１４との間で暗号通信を行う。

【００７９】

図１２は、サーバ－端末間用鍵の有効期限内に複数の情報処理装置１４と通信を行う動作を説明するためのシーケンス図である。図１２に示す場合において、それぞれの情報処理装置１４の通信条件は既に通信支援サーバ２０に登録されているものとする。情報処理装置１４－２との暗号通信に先立って、情報処理装置１４－１は、通信支援サーバ２０との間での暗号通信に用いるサーバ－端末間用鍵の共有処理を行う（Ｓ４００）。そして、情報処理装置１４－１は、情報処理装置１４－２の識別情報を通信相手の識別情報とする通信開始要求を通信支援サーバ２０へ送信する（Ｓ４０１）。

【００８０】

次に、通信支援サーバ２０は、受信した通信開始要求に含まれる情報処理装置１４－１および１４－２の識別情報に基づいて、両者に共通の通信条件を抽出する。そして、通信支援サーバ２０は、抽出した共通通信条件に基づいて、情報処理装置１４－１と情報処理装置１４－２との間の暗号通信に用いる端末－端末間用鍵１を生成する（Ｓ４０２）。そして、通信支援サーバ２０は、通信開始要求と共に、生成した端末－端末間用鍵１および当該端末－端末間用鍵１を生成するのに参照した共通通信条件を情報処理装置１４－２へ送信する（Ｓ４０３）。この場合、通信支援サーバ２０と情報処理装置１４－２との間で、有効期限内のサーバ－端末間用鍵が存在しない場合、通信支援サーバ２０と情報処理装

置１４－２との間で、ステップ４００に示したサーバー端末間用鍵の共有処理が行われる。

【００８１】

次に、情報処理装置１４－２は、通信開始要求に応じて通信開始許可を通信支援サーバ２０に応答する（Ｓ４０４）。そして、通信支援サーバ２０は、情報処理装置１４－２から受信した通信開始許可を、生成した端末－端末間用鍵１および共通通信条件と共に情報処理装置１４－１へ送信する（Ｓ４０５）。そして、情報処理装置１４－１と情報処理装置１４－２とは、通信支援サーバ２０から配布された端末－端末間用鍵１および共通通信条件を用いて互いに暗号通信を行うことができる（Ｓ４０６）。

【００８２】

ステップ４０２において、通信支援サーバ２０は、端末－端末間用鍵１と共に、当該端末－端末間用鍵１を使い続けることができる期限である有効期限を生成し、端末－端末間用鍵１および共通通信条件と共に、生成した有効期限を情報処理装置１４－１および１４－２へそれぞれ配布する。そのため、当該有効期限内であれば、ステップ４１０に示すように、情報処理装置１４－１と情報処理装置１４－２とはいつでも端末－端末間用鍵１を用いて暗号通信を行うことができる。

【００８３】

また、ステップ４００において情報処理装置１４－１と通信支援サーバ２０とが共有したサーバー端末間用鍵にも有効期限が対応付けられており、当該有効期限内であれば、情報処理装置１４－１と通信支援サーバ２０とは、ステップ４００において共有したサーバー端末間用鍵を使い続けることができる。そのため、例えば、情報処理装置１４－１が情報処理装置１４－３と暗号通信を行う場合、ステップ４００において共有したサーバー端末間用鍵の有効期限であれば、情報処理装置１４－１は、通信支援サーバ２０との鍵共有処理を省略して、ステップ４００において共有したサーバー端末間用鍵を用いて、情報処理装置１４－３への通信開始要求を暗号化して通信支援サーバ２０へ送信するステップから開始することができる（Ｓ４２０）。

【００８４】

以上のような動作により、情報処理装置１４は、複数の他の情報処理装置１４との間で暗号通信を行う場合に、それぞれの他の情報処理装置１４との間で、端末－端末間用鍵の共有処理を行う必要がなく、代わりに、通信支援サーバ２０との間で、サーバー端末間用鍵の共有処理のみを行えばよい。さらに、情報処理装置１４は、有効期限内のサーバー端末間用鍵があれば、サーバー端末間用鍵の共有処理を省略することができる。これにより、情報処理装置１４は、一度、通信支援サーバ２０との間でサーバー端末間用鍵の共有処理を行った後に、有効期限内のサーバー端末間用鍵があれば、サーバー端末間用鍵の共有処理を行うことなく、より迅速に他の情報処理装置１４との通信を開始することができる、いわゆるシングルサインオンを実現することができる。

【００８５】

図１３は、通信支援サーバ２０または情報処理装置１４を実現可能な電子計算機３０のハードウェア構成の一例を示す。電子計算機３０は、ＣＰＵ３００、ＲＡＭ３０１、ＲＯＭ３０２、外部記憶装置３０３、通信インターフェイス３０４、入出力装置３０５、およびメディアインターフェイス３０６を備える。

【００８６】

ＣＰＵ３００は、ＲＡＭ３０１およびＲＯＭ３０２に格納されたプログラムに基づいて動作し、各部の制御を行う。ＲＯＭ３０２および外部記憶装置３０３は、電子計算機３０の起動時にＣＰＵ３００が実行するブートプログラムや、電子計算機３０のハードウェアに依存するプログラム等を格納する。ＲＡＭ３０１は、ＣＰＵ３００が実行するプログラムおよびＣＰＵ３００が使用するデータ等を格納する。

【００８７】

通信インターフェイス３０４は、通信網１２を介して他の電子計算機３０から受信したプログラムおよび／またはデータを、ＲＡＭ３０１または外部記憶装置３０３に提供した

り、ＣＰＵ３００へ送ったりする。それと共に、通信インターフェイス３０４は、ＣＰＵ３００が生成したデータを他の電子計算機３０へ送信する。入出力装置３０５は、電子計算機３０の管理者やユーザからのデータを受け付けてＣＰＵ３００へ送ると共に、ＣＰＵ３００が生成したデータを管理者やユーザ等に通知する。メディアインターフェイス３０６は、記録媒体３０７からプログラムおよび／またはデータを読み取り、ＲＡＭ３０１または外部記憶装置３０３に提供する。

【００８８】

上記プログラムは、ＲＯＭ３０２または外部記憶装置３０３に予め格納されていてよい。あるいは、上記プログラムは、必要に応じて、記録媒体３０７からメディアインターフェイス３０６を介して読み出されて、ＲＯＭ３０２または外部記憶装置３０３に格納されてもよく、通信インターフェイス３０４と通信媒体とを介して、ＲＯＭ３０２または外部記憶装置３０３に格納されてもよい。

【００８９】

電子計算機３０が通信支援サーバ２０として動作する場合、電子計算機３０にインストールされて実行されるプログラムは、電子計算機３０を、暗号鍵格納部２００、鍵共有部２０２、通信条件格納部２０４、通信条件受付部２０６、暗号通信部２０８、通信開始要求受信部２１０、通信条件抽出部２１２、鍵配布制御部２１４、および鍵情報生成部２１６としてそれぞれ機能させる。

【００９０】

また、電子計算機３０が情報処理装置１４として動作する場合、電子計算機３０にインストールされて実行されるプログラムは、電子計算機３０を、鍵共有部１４０、対サーバ暗号鍵格納部１４２、対サーバ間暗号通信部１４４、通信条件登録部１４６、通信条件格納部１４８、通信開始要求送信部１５０、通信データ処理部１５２、対端末暗号鍵受信部１５４、対端末間暗号通信部１５６、および対端末暗号鍵格納部１５８としてそれぞれ機能させる。

【００９１】

記録媒体３０７は、例えばＤＶＤ、ＰＤ等の光学記録媒体、ＭＤ等の光磁気記録媒体、テープ媒体、磁気記録媒体、または半導体記録装置等であってよい。また、通信媒体は、例えばケーブル、搬送波、およびディジタル信号等であってよい。

【００９２】

以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記した実施の形態に記載の範囲には限定されない。また、上記した実施の形態に、多様な変更または改良を加えることが可能であることが当業者にとって明らかである。さらに、そのような変更または改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【００９３】

例えば、通信支援サーバ２０および情報処理装置１４が有する複数の機能ブロックのそれぞれは、ＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field Programmable Gate Array）等の集積ロジックＩＣによりハード的に実現されるものでもよく、あるいは、ＤＳＰ（Digital Signal Processor）や汎用計算機によりソフトウエア的に実現されてもよい。

【００９４】

また、本例では、通信条件格納部２０４に格納されるそれぞれの情報処理装置１４の通信条件は、それぞれの情報処理装置１４から通信網１２を介して登録されるが、他の例として、それぞれの情報処理装置１４の通信条件は、通信条件格納部２０４に予め登録されていてもよい。

【図面の簡単な説明】

【００９５】

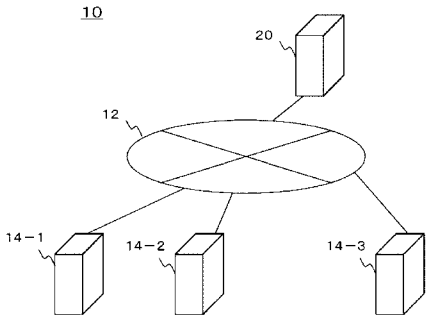
【図１】本発明の一実施形態に係る通信支援システム１０の構成を示す図である。

【図２】通信支援サーバ２０の構成の一例を示すブロック図である。

【図３】暗号鍵格納部２００に格納されるデータの構造の一例を示す図である。
【図４】通信条件格納部２０４に格納されるデータの構造の一例を示す図である。
【図５】情報処理装置１４の構成の一例を示すブロック図である。
【図６】対サーバ暗号鍵格納部１４２に格納されるデータの構造の一例を示す図である。
【図７】通信条件格納部１４８に格納されるデータの構造の一例を示す図である。
【図８】対端末暗号鍵格納部１５８に格納されるデータの構造の一例を示す図である。
【図９】通信支援サーバ２０の動作の一例を示すフローチャートである。
【図１０】情報処理装置１４が通信支援サーバ２０または他の情報処理装置１４にアクセスする場合の情報処理装置１４の動作の一例を示すフローチャートである。
【図１１】情報処理装置１４が通信支援サーバ２０または他の情報処理装置１４からアクセスされる場合の情報処理装置１４の動作の一例を示すフローチャートである。
【図１２】サーバ－端末間用鍵の有効期限内に複数の情報処理装置１４と通信を行う動作を説明するためのシーケンス図である。
【図１３】通信支援サーバ２０または情報処理装置１４を実現可能な電子計算機３０のハードウェア構成の一例を示す図である。
【符号の説明】
【００９６】
１０・・・通信支援システム、１２・・・通信網、１４・・・情報処理装置、１４０・・・鍵共有部、１４２・・・対サーバ暗号鍵格納部、１４２０、２０００、２０４０・・・識別情報、１４２２・・・サーバ－端末間用鍵、１４２４、２００４・・・有効期限、１４４・・・対サーバ間暗号通信部、１４６・・・通信条件登録部、１４８・・・通信条件格納部、１４８０・・・通信条件、１４８２・・・優先度、１５０・・・通信開始要求送信部、１５２・・・通信データ処理部、１５４・・・対端末暗号鍵受信部、１５６・・・対端末間暗号通信部、１５８・・・対端末暗号鍵格納部、２０・・・通信支援サーバ、２００・・・暗号鍵格納部、２００２・・・サーバ－端末間用鍵、２０２・・・鍵共有部、２０４・・・通信条件格納部、２０４２・・・通信条件、２０４４・・・優先度、２０６・・・通信条件受付部、２０８・・・暗号通信部、２１０・・・通信開始要求受信部、２１２・・・通信条件抽出部、２１４・・・鍵配布制御部、２１６・・・鍵情報生成部、３０・・・電子計算機、３００・・・ＣＰＵ、３０１・・・ＲＡＭ、３０２・・・ＲＯＭ、３０３・・・外部記憶装置、３０４・・・通信インターフェイス、３０５・・・入出力装置、３０６・・・メディアインターフェイス、３０７・・・記録媒体

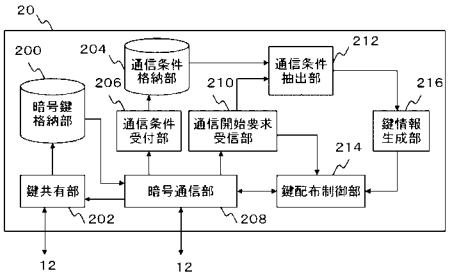
【図１】

図1



【図２】

図2



【図３】

図3

200

2000 識別情報	2002 サーバー端末間用鍵	2004 有効期限
****	********	****年**月**日 **:**:**
****	********	****年**月**日 **:**:**
⋮	⋮	⋮

【図４】

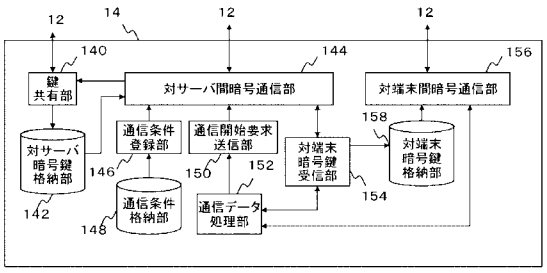
図4

204

2040 識別情報	2042－1 通信条件1	2044－1 優先度	2042－2 通信条件2	2044－2 優先度
****	********	****	********	****
****	********	****	********	****
⋮	⋮	⋮	⋮	⋮

【図５】

図5



【図６】

図6

142

1420 識別情報	1422 サーバー端末間用鍵	1424 有効期限
****	****	****年**月**日**:**:**

【図７】

図7

148

1480 通信条件	1482 優先度
********	***
********	***
⋮	⋮

【図８】

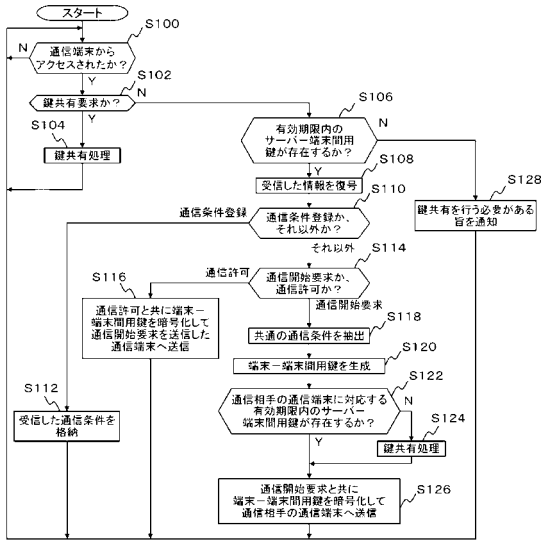
図8

158

1580 通信相手識別情報	1582 端末ー端末間用鍵	1584 共通通信条件	1586 有効期限
****	****	****	****年**月**日**:**:**
****	****	****	****年**月**日**:**:**
⋮	⋮	⋮	⋮

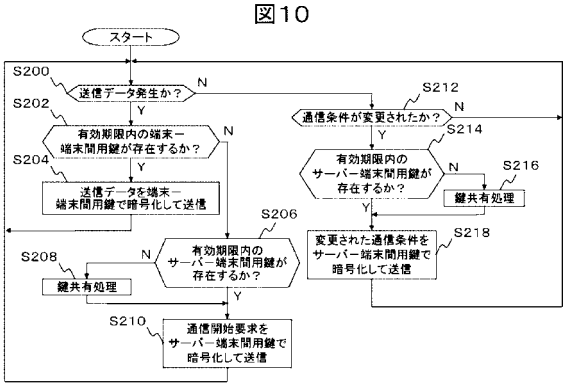
【図９】

図9



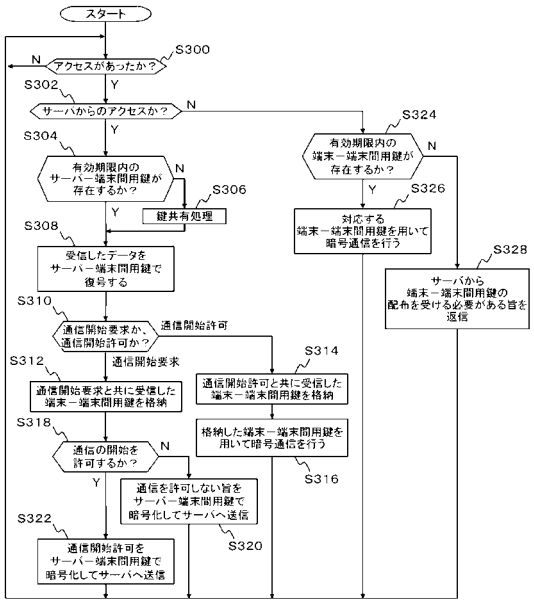
【図１０】

図10



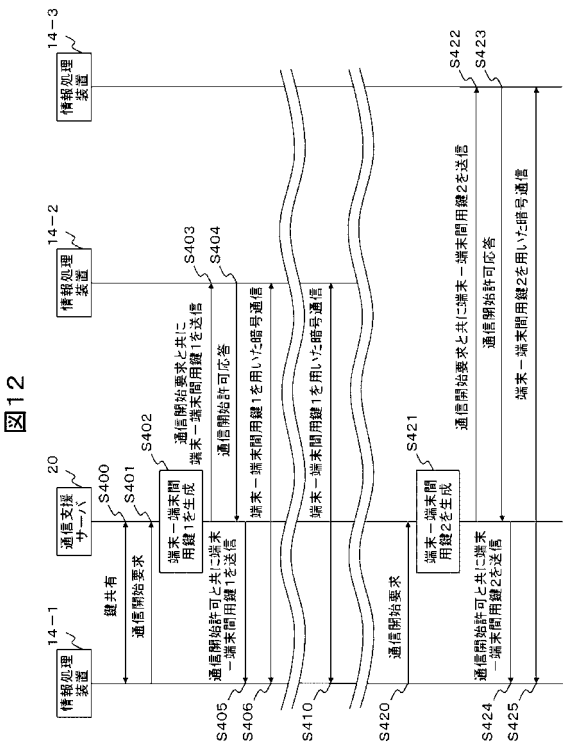
【図１１】

図11



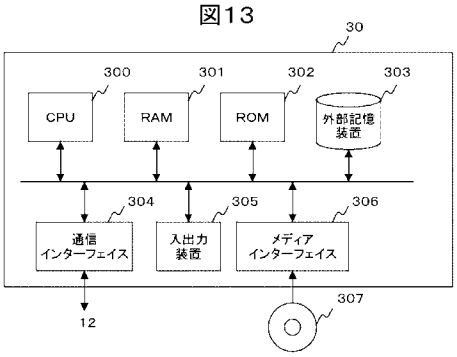
【図１２】

図12



【図１３】

図13


30
300
301
302
303
CPU
RAM
ROM
外部記憶装置
304
305
306
通信インターフェイス
入出力装置
メディアインターフェイス
12
307

フロントページの続き

(72)発明者　鍛　忠司
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　星野　和義
神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所　ネットワークソリューション事業部内

審査官　石田　信行

(56)参考文献　特開２００３－１０１５３３（ＪＰ，Ａ）
特開２００４－０５６６２８（ＪＰ，Ａ）
特開２００４－０８０５１２（ＪＰ，Ａ）
特開２００３－１７９５９２（ＪＰ，Ａ）
特開昭６３－１６１７４５（ＪＰ，Ａ）
特開２００５－３０３４８５（ＪＰ，Ａ）
特開２００４－１５９１００（ＪＰ，Ａ）
特開２００３－２４４１２３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／０８
Ｇ０９Ｃ　１／００