【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成18年8月31日(2006.8.31)

【公開番号】特開2004-159298(P2004-159298A)
【公開日】平成16年6月3日(2004.6.3)
【年通号数】公開・登録公報2004-021
【出願番号】特願2003-277898(P2003-277898)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　21/20　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｇ０６Ｆ　15/00　３３０Ｃ
Ｈ０４Ｌ　9/00　６７３Ｂ

【手続補正書】
【提出日】平成18年7月18日(2006.7.18)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ネットワーク上の他の端末装置と通信を行う端末装置であって、
当該端末装置は、前記ネットワーク上に形成されたグループの公開鍵を保持しており、
前記他の端末装置に対し、前記グループの正当なメンバか否かを問い合わせる旨を含む問合せ情報を送信する問合せ情報送信手段と、
前記他の端末装置から、前記問合せ情報に対応する応答として所定の暗号化された情報を受信する暗号化情報受信手段と、
受信された前記暗号化された情報に対し、前記グループの公開鍵で復号を試みる復号試行手段と、
前記復号試行手段において復号が成功した場合に、当該復号された情報の適否を判定する情報判定手段と、
前記復号された情報が適切であると判定された場合に、前記他の端末装置は、前記グループの正当なメンバの端末であると判定する端末判定手段と
を備えることを特徴とする端末装置。
【請求項２】
前記問合せ情報送信手段は、さらに、
前記問合せ情報に、当該端末装置を特定し得る情報を付加して送信し、
前記情報判定手段は、さらに、
前記復号された情報の中に当該端末装置を特定し得る情報が存在するか否かを含めて前記適否の判定を行う
ことを特徴とする請求項１記載の端末装置。
【請求項３】
前記問合せ情報送信手段は、さらに、
前記問合わせ情報に、前記グループへの加入を希望する旨の情報を付加して送信し、
前記情報判定手段は、さらに、
前記復号された情報の中に、前記グループへの加入を認める旨の情報が含まれているか

否かについても判定し、
前記端末判定手段は、さらに、
前記復号された情報の中に、当該端末装置の前記グループへの加入を認める旨の情報が含まれていると判定された場合に、当該端末装置は、前記グループの正当なメンバの端末であると判定する
ことを特徴とする請求項２記載の端末装置。
【請求項４】
__前記問合せ情報送信手段は、さらに、
前記問合わせ情報に、任意の文字列を付加して送信し、
前記情報判定手段は、さらに、
前記復号された情報の中に、前記文字列と前記他の端末装置の前記グループへの参加を許可する旨の参加証とが含まれているか否かについても判定し、
前記端末判定手段は、さらに、
前記復号された情報の中に、前記文字列と前記参加証が含まれていると判定された場合に、前記他の端末装置は、前記グループの正当なメンバの端末であると判定する
ことを特徴とする請求項２記載の端末装置。
【請求項５】
__前記参加証には、所定の有効期限が付加されており、
前記情報判定手段は、さらに、
前記復号された情報の中の前記参加証が、前記有効期限に基づいて有効か否かを判定し、
前記端末判定手段は、さらに、
前記参加証が有効と判定された場合に、前記他の端末装置は、前記グループの正当なメンバの端末であると判定する
ことを特徴とする請求項４記載の端末装置。
【請求項６】
__前記問合せ情報送信手段は、さらに、
前記問合わせ情報に、前記任意の文字列を付加して送信し、
前記情報判定手段は、さらに、
前記復号された情報の中に、前記文字列と所定の参加証と所定の参加証発行許可証とが含まれているか否かについても判定し、
前記端末判定手段は、さらに、
前記復号された情報の中に、前記文字列と所定の参加証と所定の参加証発行許可証とが含まれていると判定された場合に、前記他の端末装置は、前記グループの正当なメンバの端末であると判定する
ことを特徴とする請求項２記載の端末装置。
【請求項７】
__前記参加証および前記参加証発行許可証には、それぞれ所定の有効期限が付加されており、
前記情報判定手段は、さらに、
前記復号された情報の中の前記参加証および前記参加証発行許可証が、前記それぞれの有効期限に基づいて有効か否かを判定し、
前記端末判定手段は、さらに、
前記参加証および前記参加証発行許可証が共に有効と判定された場合に、前記他の端末装置は、前記グループの正当なメンバの端末であると判定する
ことを特徴とする請求項６記載の通信方法。
【請求項８】
__ネットワーク上の他の端末装置と通信を行う端末装置であって、
前記他の端末装置に対し、前記ネットワーク上に形成されたグループの公開鍵を含むグループ情報を入手したい旨を含む問合せ情報を送信する問合せ情報送信手段と、

前記他の端末装置から、前記問合せ情報に対する応答として、電子署名された前記グループ情報を受信するグループ情報受信手段と、
受信された前記グループ情報に対し、当該グループ情報に含まれる公開鍵でその正当性を検証するグループ情報検証手段と、
前記グループ情報検証手段において、前記グループ情報の正当性を確認した場合は、前記グループ情報は、前記グループの正当なメンバの端末装置から入手した情報であると判定するグループ情報判定手段と
を備えることを特徴とする端末装置。
【請求項９】
前記ネットワークは、Ｐ２Ｐネットワークである
ことを特徴とする請求項１又は８記載の端末装置。
【請求項１０】
ネットワーク上の第１の端末が、他の第２の端末と通信を行うための通信方法であって、
前記第１の端末は、前記ネットワーク上に形成されたグループの公開鍵を保持しており、
前記第２の端末に対し、前記グループの正当なメンバか否かを問い合わせる旨を含む問合せ情報を送信する問合せ情報送信ステップと、
前記第２の端末から、前記問合せ情報に対応する応答として所定の暗号化された情報を受信する暗号化情報受信ステップと、
受信された前記暗号化された情報に対し、前記グループの公開鍵で復号を試みる復号試行ステップと、
前記復号試行ステップにおいて復号が成功した場合に、当該復号された情報の適否を判定する情報判定ステップと、
前記復号された情報が適切であると判定された場合に、前記第２の端末は、前記グループの正当なメンバの端末であると判定する端末判定ステップと
を含むことを特徴とする通信方法。
【請求項１１】
ネットワーク上の第１の端末が、他の第２の端末と通信を行うための通信方法であって、
前記第２の端末に対し、前記ネットワーク上に形成されたグループの公開鍵を含むグループ情報を入手したい旨を含む問合せ情報を送信する問合せ情報送信ステップと、
前記第２の端末から、前記問合せ情報に対する応答として、電子署名された前記グループ情報を受信するグループ情報受信ステップと、
受信された前記グループ情報に対し、当該グループ情報に含まれる公開鍵でその正当性を検証するグループ情報検証ステップと、
前記グループ情報検証ステップにおいて、前記グループ情報の正当性を確認した場合は、前記グループ情報は、前記グループの正当なメンバの端末から入手した情報であると判定するグループ情報判定ステップと
を含むことを特徴とする通信方法。
【請求項１２】
ネットワーク上における第１の端末と第２の端末とで通信を行う場合の通信方法であって、
前記第１の端末は、前記ネットワーク上に形成されたグループの公開鍵と当該第１のユーザの秘密鍵及び公開鍵のペアとを保持し、前記第２の端末は、前記グループの秘密鍵及び公開鍵のペアを保持しており、
前記第１の端末では、
前記他第２の端末に対し、前記グループの正当なメンバか否かを問い合わせる旨を含む問合せ情報を送信する問合せ情報送信ステップと、
前記第２の端末から、前記問合せ情報に対する応答として所定の暗号化された情報を受

信する暗号化情報受信ステップと、
受信された前記暗号化された情報に対し、前記グループの公開鍵で復号を試みる復号試行ステップと、
前記復号試行ステップにおいて復号が成功した場合に、当該復号された情報の適否を判定する情報判定ステップと、
前記復号された情報が適切であると判定された場合に、前記第２の端末は、前記グループの正当な管理者の端末であると判定する管理者判定ステップと、
前記正当な管理者であると判定された前記第２の端末に、前記グループに加入を希望する旨を表わす情報と当該第１のユーザの公開鍵とを含む加入依頼情報を送信する加入依頼送信ステップと、
前記第２の端末から前記グループへの加入が認められた旨を表わす参加証を受信する参加証受信ステップとを含み、
前記第２の端末では、
前記第１の端末から問合せ情報を受信する問合せ情報受信ステップと、
前記受信した問合せ情報に基づいて暗号化した情報を生成して、前記第１の端末に送信する暗号化情報送信ステップと、
前記第１の端末から、前記加入依頼情報を受信する加入依頼受信ステップと、
前記受信した加入依頼情報に基づいて、前記グループへの加入を認める旨を表わす参加証を生成する参加証生成ステップと、
前記生成した参加証を前記第１の端末に送信する参加証送信ステップと
を含むことを特徴とする通信方法。
【請求項１３】
前記第２の端末では、さらに、
前記加入依頼情報を受信した年月日を特定する依頼日特定ステップと、
前記特定された年月日に基づいて、前記参加証の有効期限を決定する有効期限決定ステップとを含み、
前記参加証生成ステップでは、
前記加入依頼情報と前記有効期限とに基づいて、前記参加証を生成する
ことを特徴とする請求項１２記載の通信方法。
【請求項１４】
ネットワーク上における第１の端末と第２の端末とで通信を行う場合の通信方法であって、
前記第１の端末は、前記ネットワーク上に形成されたグループの秘密鍵及び公開鍵のペアと前記第２のユーザの公開鍵とを保持し、前記第２の端末は、前記グループの公開鍵を保持しており、
前記第１の端末では、
前記他第２の端末に対し、前記グループの正当なメンバか否かを問い合わせる旨を含む問合せ情報を送信する問合せ情報送信ステップと、
前記第２の端末から、前記問合せ情報に対する応答として所定の暗号化された情報を受信する暗号化情報受信ステップと、
受信された前記暗号化された情報に対し、前記第２のユーザの公開鍵で復号を試みる復号試行ステップと、
前記復号試行ステップにおいて復号が成功した場合に、当該復号された情報の適否を判定する情報判定ステップと、
前記復号された情報が適切であると判定された場合に、前記第２の端末は、前記グループの正当な参加者の端末であると判定する参加者判定ステップと、
前記正当な参加者であると判定された前記第２の端末に、前記グループの発行者に任命したい旨を表わす任命情報を送信する任命情報送信ステップと、
前記第２の端末から前記第２のユーザの公開鍵を受信する公開鍵受信ステップと、
前記受信した公開鍵と前記保持している公開鍵とが一致するか否かを判定する公開鍵判

定ステップと、
前記双方の公開鍵が一致すると判定された場合に、前記公開鍵を含む情報に基づいて、前記参加証を発行する権限を付与する旨を表す参加証発行許可証を作成する許可証生成ステップと、
前記作成された参加証発行許可証を前記第２の端末に送信する許可証送信ステップとを含み、
前記第２の端末では、
前記第１の端末から問合せ情報を受信する問合せ情報受信ステップと、
前記第１の端末に、当該第２のユーザの公開鍵を送信する公開鍵送信ステップと、
前記第１の端末から、前記参加証発行許可証を受信する許可証受信ステップとを含む
ことを特徴とする通信方法。
【請求項１５】
ネットワーク上における第１の端末と第２の端末とで通信を行う場合の通信方法であって、
前記第１の端末は、前記ネットワーク上に形成されたグループの公開鍵と当該第１のユーザの秘密鍵及び公開鍵のペアとを保持し、前記第２の端末は、前記グループの公開鍵を保持しており、
前記第１の端末では、
前記他第２の端末に対し、前記グループの正当な発行者か否かを問い合わせる旨を含む問合せ情報を送信する問合せ情報送信ステップと、
前記第２の端末から、暗号化された参加証発行許可証を受信する許可証受信ステップと、
受信された前記参加証発行許可証に対し、前記グループの公開鍵で復号を試みる復号試行ステップと、
前記復号試行ステップにおいて復号が成功した場合に、当該復号された情報の適否を判定する情報判定ステップと、
前記復号された情報が適切であると判定された場合に、前記第２の端末は、前記グループの正当な発行者の端末であると判定する発行者判定ステップと、
前記正当な発行者であると判定された前記第２の端末に、前記グループに加入を希望する旨を表わす情報と当該第１のユーザの公開鍵とを含む加入依頼情報を送信する加入依頼送信ステップと、
前記第２の端末から前記グループへの加入が認められた旨を表わす参加証を受信する参加証受信ステップとを含み、
前記第２の端末では、
前記第１の端末から問合せ情報を受信する問合せ情報受信ステップと、
前記問合せ情報を受信後に、参加証発行許可証を前記第１の端末に送信する暗号化情報送信ステップと、
前記第１の端末から、前記加入依頼情報を受信する加入依頼受信ステップと、
前記受信した加入依頼情報に基づいて、前記グループへの加入を認める旨を表わす参加証を生成する参加証生成ステップと、
前記生成した参加証を前記第１の端末に送信する参加証送信ステップと
を含むことを特徴とする通信方法。
【請求項１６】
前記ネットワークは、Ｐ２Ｐネットワークである
ことを特徴とする請求項１２、１４又は１５記載の通信方法。
【請求項１７】
ネットワーク上における第１の端末と第２の端末とで通信を行う通信システムであって、
前記第１の端末は、前記ネットワーク上に形成されたグループの公開鍵と当該第１のユーザの秘密鍵及び公開鍵のペアとを保持し、前記第２の端末は、前記グループの秘密鍵及

び公開鍵のペアを保持しており、
前記第１の端末は、
前記他第２の端末に対し、前記グループの正当なメンバか否かを問い合わせる旨を含む問合せ情報を送信する問合せ情報送信手段と、
前記第２の端末から、前記問合せ情報に対する応答として所定の暗号化された情報を受信する暗号化情報受信手段と、
受信された前記暗号化された情報に対し、前記グループの公開鍵で復号を試みる復号試行手段と、
前記復号試行手段において復号が成功した場合に、当該復号された情報の適否を判定する情報判定手段と、
前記復号された情報が適切であると判定された場合に、前記第２の端末は、前記グループの正当な管理者の端末であると判定する管理者判定手段と、
前記正当な管理者であると判定された前記第２の端末に、前記グループに加入を希望する旨を表わす情報と当該第１のユーザの公開鍵とを含む加入依頼情報を送信する加入依頼送信手段と、
前記第２の端末から前記グループへの加入が認められた旨を表わす参加証を受信する参加証受信手段とを備え、
前記第２の端末は、
前記第１の端末から問合せ情報を受信する問合せ情報受信手段と、
前記受信した問合せ情報に基づいて暗号化した情報を生成して、前記第１の端末に送信する暗号化情報送信手段と、
前記第１の端末から、前記加入依頼情報を受信する加入依頼受信手段と、
前記受信した加入依頼情報に基づいて、前記グループへの加入を認める旨を表わす参加証を生成する参加証生成手段と、
前記生成した参加証を前記第１の端末に送信する参加証送信手段と
を備えることを特徴とする通信システム。
【請求項１８】
ネットワーク上における第１の端末と第２の端末とで通信を行う通信システムであって、
前記第１の端末は、前記ネットワーク上に形成されたグループの秘密鍵及び公開鍵のペアと前記第２のユーザの公開鍵とを保持し、前記第２の端末は、前記グループの公開鍵を保持しており、
前記第１の端末は、
前記他第２の端末に対し、前記グループの正当なメンバか否かを問い合わせる旨を含む問合せ情報を送信する問合せ情報送信手段と、
前記第２の端末から、前記問合せ情報に対する応答として所定の暗号化された情報を受信する暗号化情報受信手段と、
受信された前記暗号化された情報に対し、前記第２のユーザの公開鍵で復号を試みる復号試行手段と、
前記復号試行手段において復号が成功した場合に、当該復号された情報の適否を判定する情報判定手段と、
前記復号された情報が適切であると判定された場合に、前記第２の端末は、前記グループの正当な参加者の端末であると判定する参加者判定手段と、
前記正当な参加者であると判定された前記第２の端末に、前記グループの発行者に任命したい旨を表わす任命情報を送信する任命情報送信手段と、
前記第２の端末から前記第２のユーザの公開鍵を受信する公開鍵受信手段と、
前記受信した公開鍵と前記保持している公開鍵とが一致するか否かを判定する公開鍵判定手段と、
前記双方の公開鍵が一致すると判定された場合に、前記公開鍵を含む情報に基づいて、前記参加証を発行する権限を付与する旨を表す参加証発行許可証を作成する許可証生成手

段と、
前記作成された参加証発行許可証を前記第２の端末に送信する許可証送信手段とを備え、
前記第２の端末は、
前記第１の端末から問合せ情報を受信する問合せ情報受信手段と、
前記第１の端末に、当該第２のユーザの公開鍵を送信する公開鍵送信手段と、
前記第１の端末から、前記参加証発行許可証を受信する許可証受信手段と
を備えることを特徴とする通信システム。
【請求項１９】
ネットワーク上における第１の端末と第２の端末とで通信を行う通信システムであって、
前記第１の端末は、前記ネットワーク上に形成されたグループの公開鍵と当該第１のユーザの秘密鍵及び公開鍵のペアとを保持し、前記第２の端末は、前記グループの公開鍵を保持しており、
前記第１の端末は、
前記他第２の端末に対し、前記グループの正当な発行者か否かを問い合わせる旨を含む問合せ情報を送信する問合せ情報送信手段と、
前記第２の端末から、暗号化された参加証発行許可証を受信する許可証受信手段と、
受信された前記参加証発行許可証に対し、前記グループの公開鍵で復号を試みる復号試行手段と、
前記復号試行手段において復号が成功した場合に、当該復号された情報の適否を判定する情報判定手段と、
前記復号された情報が適切であると判定された場合に、前記第２の端末は、前記グループの正当な発行者の端末であると判定する発行者判定手段と、
前記正当な発行者であると判定された前記第２の端末に、前記グループに加入を希望する旨を表わす情報と当該第１のユーザの公開鍵とを含む加入依頼情報を送信する加入依頼送信手段と、
前記第２の端末から前記グループへの加入が認められた旨を表わす参加証を受信する参加証受信手段とを備え、
前記第２の端末は、
前記第１の端末から問合せ情報を受信する問合せ情報受信手段と、
前記問合せ情報を受信後に、参加証発行許可証を前記第１の端末に送信する暗号化情報送信手段と、
前記第１の端末から、前記加入依頼情報を受信する加入依頼受信手段と、
前記受信した加入依頼情報に基づいて、前記グループへの加入を認める旨を表わす参加証を生成する参加証生成手段と、
前記生成した参加証を前記第１の端末に送信する参加証送信手段と
を備えることを特徴とする通信システム。
【請求項２０】
ネットワーク上の他の端末装置と通信を行う端末装置に用いる、コンピュータに実行させるためのプログラムであって、
当該端末装置は、前記ネットワーク上に形成されたグループの公開鍵を保持しており、
前記他の端末装置に対し、前記グループの正当なメンバか否かを問い合わせる旨を含む問合せ情報を送信する問合せ情報送信ステップと、
前記他の端末装置から、前記問合せ情報に対する応答として所定の暗号化された情報を受信する暗号化情報受信ステップと、
受信された前記暗号化された情報に対し、前記グループの公開鍵で復号を試みる復号試行ステップと、
前記復号試行ステップにおいて復号が成功した場合に、当該復号された情報の適否を判定する情報判定ステップと、

前記復号された情報が適切であると判定された場合に、前記他の端末装置は、前記グループの正当なメンバの端末であると判定する端末判定ステップと
を含むことを特徴とするプログラム。