

請求の範囲

- [請求項1] クライアント装置とネットワーク通信網とに接続される第1の通信制御装置と、
- サーバ装置とネットワーク通信網とに接続される第2の通信制御装置と、
- を備え、
- 前記第1の通信制御装置は、
- 第1の認証部と、
- 前記第1の認証部に、プライベート認証局により発行された秘密鍵、及びクライアント証明書を用いる相互認証を前記第2の通信制御装置との通信において行う第1の相互認証処理と、前記第1の相互認証処理により決定された共通鍵を用いて前記クライアント装置により前記サーバ装置に対して送信される情報を暗号化するとともに、前記サーバ装置により前記クライアント装置に対して送信された情報を復号する第1の暗号化復号処理とのうち少なくとも一方の処理を依頼し、
- 前記第1の認証部に前記第1の暗号化復号処理を依頼した場合、前記暗号化された情報を前記第2の通信制御装置に送信し、前記復号された情報を前記クライアント装置に送信する第1の制御部を有し、
- 前記第2の通信制御装置は、
- 第2の認証部と、
- 前記第2の認証部に、前記プライベート認証局により発行された秘密鍵、及びサーバ証明書を用いる相互認証を前記第1の通信制御装置との通信において行う第2の相互認証処理と、前記第2の相互認証処理により決定された共通鍵を用いて前記サーバ装置により前記クライアント装置に対して送信される情報を暗号化するとともに、前記クライアント装置により前記サーバ装置に対して送信された情報を復号する第2の暗号化復号処理とのうち少なくとも一方の処理を依頼し、
- 前記第2の認証部に前記第2の暗号化復号処理を依頼した場合、前記

暗号化された情報を前記第 1 の通信制御装置に送信し、前記復号された情報を前記サーバ装置に送信する第 2 の制御部を有する

通信制御システム。

[請求項2] 前記第 1 の認証部は、前記第 1 の通信制御装置に対して着脱可能に装着される

請求項 1 に記載の通信制御システム。

[請求項3] 前記プライベート認証局を更に備え、
前記プライベート認証局は、前記第 1 の認証部に記憶させる秘密鍵、及びクライアント証明書を前記第 1 の通信制御装置に送信し、前記第 2 の認証部に記憶させる秘密鍵、及びサーバ証明書を前記第 2 の通信制御装置に送信する

請求項 1 又は請求項 2 に記載の通信制御システム。

[請求項4] 前記第 1 の制御部は、前記相互認証を前記クライアント装置に対して情報を送信した通信装置との通信において行うように前記第 1 の認証部に依頼し、前記相互認証の結果に基づいて前記通信装置に対して前記クライアント装置との通信を許可するか否かを判定し、判定結果を前記プライベート認証局に送信する

請求項 1 から請求項 3 のいずれか一項に記載の通信制御システム。

[請求項5] 前記第 1 の制御部は、前記クライアント装置に対して送信された前記クライアント装置のファームウェアに関する情報の内容が正しいか否かの検証を前記プライベート認証局により発行された鍵を用いて行うファームウェア検証処理を前記第 1 の認証部に依頼する

請求項 1 から請求項 4 のいずれか一項に記載の通信制御システム。

[請求項6] 前記第 1 の認証部は、前記クライアント装置に対する通信が許可される通信機器に関する情報を示す送信先リストに基づいて、前記クライアント装置に対して情報を送信した通信装置に対する前記クライアント装置との通信を許可するか否かを判定する

請求項 1 から請求項 5 のいずれか一項に記載の通信制御システム。

- [請求項7] 前記プライベート認証局は、前記クライアント証明書の有効期限に基づいて、前記クライアント証明書を更新する証明書更新部を更に備え、
- 前記プライベート認証局は、前記証明書更新部により更新された前記クライアント証明書を前記第1の通信制御装置に送信する
- 請求項3に記載の通信制御システム。
- [請求項8] 前記プライベート認証局は、前記第1の通信制御装置による前記第1の相互認証処理において、相互に正当性が証明されなかった場合、前記クライアント証明書を無効化する管理部を更に備える
- 請求項3又は請求項7に記載の通信制御システム。
- [請求項9] 前記第1の通信制御装置は、所定のタイミングで前記クライアント装置との接続が維持されているか否かを判定する
- 請求項1から請求項8のいずれか一項に記載の通信制御システム。
- [請求項10] 第1の通信装置とネットワーク通信網とに接続される通信制御装置であって、
- 認証部と、
- 前記認証部に、プライベート認証局により発行された秘密鍵、及び証明書を用いる相互認証を他の通信制御装置との通信において行う相互認証処理と、前記相互認証処理により決定された共通鍵を用いて前記第1の通信装置により、前記第1の通信装置の通信先である第2の通信装置に対して送信される情報を暗号化するとともに、前記第2の通信装置により前記第1の通信装置に対して送信された情報を復号する暗号化復号処理とのうち少なくとも一方の処理を依頼し、前記認証部に前記暗号化復号処理を依頼した場合、前記暗号化された情報を前記他の通信制御装置に送信し、前記復号された情報を前記第1の通信装置に送信する制御部と
- を有する通信制御装置。