

【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 28 年 3 月 24 日 (2016.3.24)

【公開番号】特開 2014-168204 (P2014-168204A)

【公開日】平成 26 年 9 月 11 日 (2014.9.11)

【年通号数】公開・登録公報 2014-049

【出願番号】特願 2013-40032 (P2013-40032)

【国際特許分類】

H 0 4 L 9/36 (2006.01)

H 0 4 L 9/08 (2006.01)

H 0 4 L 12/28 (2006.01)

【F I】

H 0 4 L 9/00 6 8 5

H 0 4 L 9/00 6 0 1 B

H 0 4 L 9/00 6 0 1 E

H 0 4 L 12/28 2 0 0 Z

【手続補正書】

【提出日】平成 28 年 2 月 3 日 (2016.2.3)

【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】

所定のセキュリティが確保されていないセッションにおける送信データを生成する生成手段と、

前記生成手段により前記送信データが生成された場合に、当該セッションの相手装置が該セッションに対応する前記所定のセキュリティを確保するための第 1 の処理を開始しているかを判定する判定手段と、

前記判定手段により、前記第 1 の処理が開始されていないと判定された場合に、前記所定のセキュリティを確保するための第 2 の処理を開始する開始手段と、

前記判定手段により、前記第 1 の処理が開始されていると判定された場合、当該第 1 の処理により前記所定のセキュリティが確保されたことに応じて、前記第 1 の処理により確保された前記所定のセキュリティを用いて、前記送信データを送信し、

前記判定手段により、前記第 1 の処理が開始されていないと判定された場合、前記第 2 の処理により前記所定のセキュリティが確保されたことに応じて、前記第 2 の処理により確保された前記所定のセキュリティを用いて、前記送信データを送信する送信手段と、
を有することを特徴とする通信装置。

【請求項 2】

前記生成手段により生成された前記送信データを前記セッションと対応付けて管理する管理手段をさらに有する、

ことを特徴とする請求項 1 に記載の通信装置。

【請求項 3】

前記第 1 の処理は、前記セッションの相手装置が開始した鍵交換処理であり、

前記第 2 の処理は、前記通信装置が開始した鍵交換処理である、

ことを特徴とする請求項 1 または 2 に記載の通信装置。

【請求項 4】

前記第 1 の処理または前記第 2 の処理によって交換された鍵を用いて、前記送信データを暗号化する暗号化手段をさらに有し、

前記送信手段は、前記暗号化手段により暗号化された前記送信データを送信する、
ことを特徴とする請求項 1 から 3 のいずれか 1 項に記載の通信装置。

【請求項 5】

前記第 1 の処理、および、前記第 2 の処理は、IKE (Internet Key Exchange) プロトコルに準拠した処理である、

ことを特徴とする請求項 1 から 4 のいずれか 1 項に記載の通信装置。

【請求項 6】

前記判定手段により、前記第 1 の処理が開始されていると判定された場合、前記開始手段は、前記第 2 の処理を開始しない、

ことを特徴とする請求項 1 から 5 のいずれか 1 項に記載の通信装置。

【請求項 7】

前記判定手段により、前記第 1 の処理が開始されていると判定された場合において、前記第 1 の処理による前記所定のセキュリティの確保が失敗した場合、前記送信データを破棄する第 1 の破棄手段をさらに有する、

ことを特徴とする請求項 1 から 6 のいずれか 1 項に記載の通信装置。

【請求項 8】

前記判定手段により、前記第 1 の処理が開始されていないと判定された場合において、前記第 2 の処理による前記所定のセキュリティの確保が失敗した場合、前記送信データを破棄する第 2 の破棄手段をさらに有する、

ことを特徴とする請求項 1 から 7 のいずれか 1 項に記載の通信装置。

【請求項 9】

所定のセキュリティが確保されていないセッションにおける送信データを生成する生成工程と、

前記送信データが生成された場合に、当該セッションの相手装置が該セッションに対応する前記所定のセキュリティを確保するための第 1 の処理を開始しているかを判定する判定工程と、

前記第 1 の処理が開始されていないと判定された場合に、前記所定のセキュリティを確保するための第 2 の処理を開始する開始工程と、

前記第 1 の処理が開始されていると判定された場合、当該第 1 の処理により前記所定のセキュリティが確保されたことに応じて、前記第 1 の処理により確保された前記所定のセキュリティを用いて、前記送信データを送信する第 1 の送信工程と、

前記第 1 の処理が開始されていないと判定された場合、前記第 2 の処理により前記所定のセキュリティが確保されたことに応じて、前記第 2 の処理により確保された前記所定のセキュリティを用いて、前記送信データを送信する第 2 の送信工程と、

を有することを特徴とする通信方法。

【請求項 10】

コンピュータを請求項 1 から 8 のいずれか 1 項に記載の通信装置として動作させるためのプログラム。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正の内容】

【0011】

上記目的を達成するため、本発明による通信装置は、所定のセキュリティが確保されていないセッションにおける送信データを生成する生成手段と、前記生成手段により前記送信データが生成された場合に、当該セッションの相手装置が該セッションに対応する前記所定のセキュリティを確保するための第 1 の処理を開始しているかを判定する判定手段と

、前記判定手段により、前記第１の処理が開始されていないと判定された場合に、前記所定のセキュリティを確保するための第２の処理を開始する開始手段と、前記判定手段により、前記第１の処理が開始されていると判定された場合、当該第１の処理により前記所定のセキュリティが確保されたことに応じて、前記第１の処理により確保された前記所定のセキュリティを用いて、前記送信データを送信し、前記判定手段により、前記第１の処理が開始されていないと判定された場合、前記第２の処理により前記所定のセキュリティが確保されたことに応じて、前記第２の処理により確保された前記所定のセキュリティを用いて、前記送信データを送信する送信手段と、を有する。