【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17年7月14日(2005.7.14)

【公開番号】特開2003-152699(P2003-152699A)
【公開日】平成15年5月23日(2003.5.23)
【出願番号】特願2001-349648(P2001-349648)
【国際特許分類第７版】
　ＨＯ４Ｌ　9/08
　ＨＯ４Ｌ　9/32
【ＦＩ】
　ＨＯ４Ｌ　9/00　６０１Ｃ
　ＨＯ４Ｌ　9/00　６０１Ｅ
　ＨＯ４Ｌ　9/00　６７５Ａ

【手続補正書】
【提出日】平成16年11月15日(2004.11.15)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正の内容】
【発明の名称】情報処理システムおよび情報処理方法
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
　データを送受信する携帯型情報端末装置と、前記データを送受信する第１の情報処理装置と、ネットワークを介して前記第１の情報処理装置と前記データを送受信する第２の情報処理装置とからなる情報処理システムにおいて、
　前記携帯型情報端末装置は、
　　情報記憶媒体と接続し、前記情報記憶媒体を認証する第１の認証手段と、
　　前記第１の認証手段により前記情報記憶媒体が認証されたとき、前記データを暗号化して前記情報記憶媒体に記憶する記憶手段と
　を備え、
　前記第１の情報処理装置は、
　　前記情報記憶媒体と接続し、前記情報記憶媒体を認証する第２の認証手段と、
　　前記第２の認証手段により前記情報記憶媒体が認証されたとき、前記情報記憶媒体に記憶されている前記データを読み出して復号する読み出し手段と、
　　前記第２の情報処理装置と前記ネットワークを介して接続し、前記第２の情報処理装置を認証する第３の認証手段と、
　　前記第３の認証手段により前記第２の情報処理装置が認証されたとき、前記読み出し手段により読み出された前記データを暗号化して、前記ネットワークを介して前記第２の情報処理装置に送信する送信手段と
　を備え、
　前記第２の情報処理装置は、
　　前記第３の認証手段により前記第１の情報処理装置が認証されたとき、前記ネットワ

ークを介して前記第１の情報処理装置より送信されてくる前記データを受信する受信手段と
を備えることを特徴とする情報処理システム。
【請求項２】
前記携帯型情報端末装置は、
前記第１の認証手段により生成された一時鍵で前記データを暗号化する
ことを特徴とする請求項１に記載の情報処理システム。
【請求項３】
前記第１の情報処理装置は、
前記第２の認証手段により生成された第１の一時鍵で前記データを復号し、
前記第３の認証手段により生成された第２の一時鍵で前記データを暗号化する
ことを特徴とする請求項１に記載の情報処理システム。
【請求項４】
前記第２の情報処理装置は、
前記第３の認証手段により生成された一時鍵で、前記受信手段により受信された前記データを復号する復号手段をさらに備える
ことを特徴とする請求項１に記載の情報処理システム。
【請求項５】
前記ネットワークは、ブロードバンドネットワークである
ことを特徴とする請求項１に記載の情報処理システム。
【請求項６】
データを送受信する携帯型情報端末装置と、前記データを送受信する第１の情報処理装置と、ネットワークを介して前記第１の情報処理装置と前記データを送受信する第２の情報処理装置とからなる情報処理システムの情報処理方法において、
前記携帯型情報端末装置は、
情報記憶媒体と接続し、前記情報記憶媒体を認証する第１の認証ステップと、
前記第１の認証ステップの処理により前記情報記憶媒体が認証されたとき、前記データを暗号化して前記情報記憶媒体に記憶するよう制御する記憶制御ステップと
を含み、
前記第１の情報処理装置は、
前記情報記憶媒体と接続し、前記情報記憶媒体を認証する第２の認証ステップと、
前記第２の認証ステップにより前記情報記憶媒体が認証されたとき、前記情報記憶媒体に記憶されている前記データを読み出して復号する読み出しステップと、
前記第２の情報処理装置と前記ネットワークを介して接続し、前記第２の情報処理装置を認証する第３の認証ステップと、
前記第３の認証ステップにより前記第２の情報処理装置が認証されたとき、前記読み出しステップの処理により読み出された前記データを暗号化して、前記ネットワークを介して前記第２の情報処理装置に送信する送信ステップと
を含み、
前記第２の情報処理装置は、
前記第３の認証ステップの処理により前記第１の情報処理装置が認証されたとき、前記ネットワークを介して前記第１の情報処理装置より送信されてくる前記データを受信する受信ステップと
を含むことを特徴とする情報処理方法。
【請求項７】
前記携帯型情報端末装置は、
前記第１の認証ステップの処理により生成された一時鍵で前記データを暗号化する
ことを特徴とする請求項６に記載の情報処理方法。
【請求項８】
前記第１の情報処理装置は、

前記第２の認証ステップの処理により生成された第１の一時鍵で前記データを復号し、
前記第３の認証ステップの処理により生成された第２の一時鍵で前記データを暗号化する
ことを特徴とする請求項６に記載の情報処理方法。
【請求項９】
前記第２の情報処理装置は、
前記第３の認証ステップの処理により生成された一時鍵で、前記受信ステップの処理により受信された前記データを復号する復号ステップをさらに含む
ことを特徴とする請求項６に記載の情報処理方法。
【請求項１０】
前記ネットワークは、ブロードバンドネットワークである
ことを特徴とする請求項６に記載の情報処理方法。
【請求項１１】
携帯型情報端末装置と、前記携帯型情報端末装置との間で、情報記憶媒体を介してデータを授受する情報処理装置からなる情報処理システムにおいて、
前記携帯型情報端末装置は、
前記データを記憶する第１の記憶手段と、
接続が確立された前記情報記憶媒体を認証する第１の認証手段と、
前記第１の認証手段により前記情報記憶媒体が認証された場合、前記第１の記憶手段に記憶されている前記データを暗号化する第１の暗号化手段と、
前記第１の暗号化手段により暗号化された前記データを、前記情報記憶媒体に書き込む書き込み手段と
を備え、
前記情報処理装置は、
接続が確立された前記情報記憶媒体を認証する第２の認証手段と、
前記第２の認証手段により前記情報記憶媒体が認証された場合、前記情報記憶媒体から、暗号化された前記データを読み出す読み出し手段と、
前記読み出し手段により読み出された暗号化された前記データを復号する復号手段と、
前記復号手段により復号された前記データを記憶する第２の記憶手段と、
接続が確立された他の情報処理装置を認証する第３の認証手段と、
前記第３の認証手段により前記他の情報処理装置が認証された場合、前記第２の記憶手段に記憶されている前記データを暗号化する第２の暗号化手段と、
前記第２の暗号化手段により暗号化された前記データを、ネットワークを介して前記他の情報処理装置に送信する送信手段と
を備えることを特徴とする情報処理システム。
【請求項１２】
前記第１の認証手段は、前記情報記憶媒体を認証した場合、前記情報記憶媒体との間で第１の暗号鍵を共有し、
前記第１の暗号化手段は、前記第１の暗号鍵を用いて前記データを暗号化し、
前記第２の認証手段は、前記情報記憶媒体を認証した場合、前記情報記憶媒体との間で第２の暗号鍵を共有し、
前記復号手段は、前記第２の暗号鍵を用いて暗号化された前記データを復号し、
前記第３の認証手段は、前記他の情報処理装置を認証した場合、前記他の情報処理装置との間で第３の暗号鍵を共有し、
前記第２の暗号化手段は、前記第３の暗号鍵を用いて前記データを暗号化する
ことを特徴とする請求項１１に記載の情報処理システム。
【請求項１３】
携帯型情報端末装置と、前記携帯型情報端末装置との間で、情報記憶媒体を介してデータを授受する情報処理装置からなる情報処理システムの情報処理方法において、

前記携帯型情報端末装置は、
接続が確立された前記情報記憶媒体を認証する第１の認証ステップと、
前記第１の認証ステップの処理により前記情報記憶媒体が認証された場合、第１の記憶部に記憶されている前記データを暗号化する第１の暗号化ステップと、
前記第１の暗号化ステップの処理により暗号化された前記データを、前記情報記憶媒体に書き込む書き込みステップと
を含み、
前記情報処理装置は、
接続が確立された前記情報記憶媒体を認証する第２の認証ステップと、
前記第２の認証ステップの処理により前記情報記憶媒体が認証された場合、前記情報記憶媒体から、暗号化された前記データを読み出す読み出しステップと、
前記読み出しステップの処理により読み出された暗号化された前記データを復号する復号ステップと、
前記復号ステップの処理により復号された前記データの第２の記憶部への記憶を制御する記憶制御ステップと、
接続が確立された他の情報処理装置を認証する第３の認証ステップと、
前記第３の認証ステップの処理により前記他の情報処理装置が認証された場合、前記第２の記憶部に記憶されている前記データを暗号化する第２の暗号化ステップと、
前記第２の暗号化ステップの処理により暗号化された前記データを、ネットワークを介して前記他の情報処理装置に送信する送信ステップと
を含むことを特徴とする情報処理方法。
【請求項１４】
前記第１の認証ステップの処理では、前記情報記憶媒体を認証した場合、前記情報記憶媒体との間で第１の暗号鍵を共有し、
前記第１の暗号化ステップの処理では、前記第１の暗号鍵を用いて前記データを暗号化し、
前記第２の認証ステップの処理では、前記情報記憶媒体を認証した場合、前記情報記憶媒体との間で第２の暗号鍵を共有し、
前記復号ステップの処理では、前記第２の暗号鍵を用いて暗号化された前記データを復号し、
前記第３の認証ステップの処理では、前記他の情報処理装置を認証した場合、前記他の情報処理装置との間で第３の暗号鍵を共有し、
前記第２の暗号化ステップの処理では、前記第３の暗号鍵を用いて前記データを暗号化する
ことを特徴とする請求項１３に記載の情報処理方法。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００１
【補正方法】変更
【補正の内容】
【０００１】
【発明の属する技術分野】
本発明は、情報処理システムおよび情報処理方法に関し、特に、例えば、PDA（Personal Digital Assistant）などの携帯型情報端末装置とサーバとのデータ通信において、広帯域で秘匿性の高い通信路を確立するようにした情報処理システムおよび情報処理方法に関する。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更

【補正の内容】
【００２３】
【課題を解決するための手段】
本発明の第１の情報処理システムは、携帯型情報端末装置が、情報記憶媒体と接続し、情報記憶媒体を認証する第１の認証手段と、第１の認証手段により情報記憶媒体が認証されたとき、データを暗号化して情報記憶媒体に記憶する記憶手段とを備え、第１の情報処理装置が、情報記憶媒体と接続し、情報記憶媒体を認証する第２の認証手段と、第２の認証手段により情報記憶媒体が認証されたとき、情報記憶媒体に記憶されているデータを読み出して復号する読み出し手段と、第２の情報処理装置とネットワークを介して接続し、第２の情報処理装置を認証する第３の認証手段と、第３の認証手段により第２の情報処理装置が認証されたとき、読み出し手段により読み出されたデータを暗号化して、ネットワークを介して第２の情報処理装置に送信する送信手段とを備え、第２の情報処理装置が、第３の認証手段により第１の情報処理装置が認証されたとき、ネットワークを介して第１の情報処理装置より送信されてくるデータを受信する受信手段とを備えることを特徴とする。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】変更
【補正の内容】
【００２８】
本発明の第１の情報処理方法は、携帯型情報端末装置が、情報記憶媒体と接続し、情報記憶媒体を認証する第１の認証ステップと、第１の認証ステップの処理により情報記憶媒体が認証されたとき、データを暗号化して情報記憶媒体に記憶するよう制御する記憶制御ステップとを含み、第１の情報処理装置が、情報記憶媒体と接続し、情報記憶媒体を認証する第２の認証ステップと、第２の認証ステップにより情報記憶媒体が認証されたとき、情報記憶媒体に記憶されているデータを読み出して復号する読み出しステップと、第２の情報処理装置とネットワークを介して接続し、第２の情報処理装置を認証する第３の認証ステップと、第３の認証ステップにより第２の情報処理装置が認証されたとき、読み出しステップの処理により読み出されたデータを暗号化して、ネットワークを介して第２の情報処理装置に送信する送信ステップとを含み、第２の情報処理装置が、第３の認証ステップの処理により第１の情報処理装置が認証されたとき、ネットワークを介して第１の情報処理装置より送信されてくるデータを受信する受信ステップとを含むことを特徴とする。
携帯型情報端末装置は、第１の認証ステップの処理により生成された一時鍵でデータを暗号化することができる。
第１の情報処理装置は、第２の認証ステップの処理により生成された第１の一時鍵でデータを復号し、第３の認証の認証ステップの処理により生成された第２の一時鍵でデータを暗号化することができる。
第２の情報処理装置は、第３の認証ステップの処理により生成された一時鍵で、受信ステップの処理により受信されたデータを復号する復号ステップをさらに含むことができる。
ネットワークは、ブロードバンドネットワークであるものとすることができる。
第１の本発明においては、携帯型情報端末装置で、情報記憶媒体と認証されたとき、データを暗号化して情報記憶媒体に記憶させ、第１の情報処理装置で、情報記憶媒体と認証されたとき、情報記憶媒体に記憶されているデータが読み出されて復号され、第２の情報処理装置とネットワークを介して認証されたとき、読み出されたデータが暗号化されてネットワークを介して第２の情報処理装置に送信され、第２の情報処理装置で、第１の情報処理装置と認証されたとき、ネットワークを介して第１の情報処理装置より送信されてくるデータが受信される。
本発明の第２の情報処理装置は、携帯型情報端末装置が、データを記憶する第１の記憶

手段と、接続が確立された情報記憶媒体を認証する第１の認証手段と、第１の認証手段により情報記憶媒体が認証された場合、第１の記憶手段に記憶されているデータを暗号化する第１の暗号化手段と、第１の暗号化手段により暗号化されたデータを、情報記憶媒体に書き込む書き込み手段とを備え、情報処理装置が、接続が確立された情報記憶媒体を認証する第２の認証手段と、第２の認証手段により情報記憶媒体が認証された場合、情報記憶媒体から、暗号化されたデータを読み出す読み出し手段と、読み出し手段により読み出された暗号化されたデータを復号する復号手段と、復号手段により復号されたデータを記憶する第２の記憶手段と、接続が確立された他の情報処理装置を認証する第３の認証手段と、第３の認証手段により他の情報処理装置が認証された場合、第２の記憶手段に記憶されているデータを暗号化する第２の暗号化手段と、第２の暗号化手段により暗号化されたデータを、ネットワークを介して他の情報処理装置に送信する送信手段とを備えることを特徴とする。

第１の認証手段は、情報記憶媒体を認証した場合、情報記憶媒体との間で第１の暗号鍵を共有し、第１の暗号化手段は、第１の暗号鍵を用いてデータを暗号化し、第２の認証手段は、情報記憶媒体を認証した場合、情報記憶媒体との間で第２の暗号鍵を共有し、復号手段は、第２の暗号鍵を用いて暗号化されたデータを復号し、第３の認証手段は、他の情報処理装置を認証した場合、他の情報処理装置との間で第３の暗号鍵を共有し、第２の暗号化手段は、第３の暗号鍵を用いてデータを暗号化するものとすることができる。

本発明の第２の情報処理方法は、携帯型情報端末装置が、接続が確立された情報記憶媒体を認証する第１の認証ステップと、第１の認証ステップの処理により情報記憶媒体が認証された場合、第１の記憶部に記憶されているデータを暗号化する第１の暗号化ステップと、第１の暗号化ステップの処理により暗号化されたデータを、情報記憶媒体に書き込む書き込みステップとを含み、情報処理装置が、接続が確立された情報記憶媒体を認証する第２の認証ステップと、第２の認証ステップの処理により情報記憶媒体が認証された場合、情報記憶媒体から、暗号化されたデータを読み出す読み出しステップと、読み出しステップの処理により読み出された暗号化されたデータを復号する復号ステップと、復号ステップの処理により復号されたデータの第２の記憶部への記憶を制御する記憶制御ステップと、接続が確立された他の情報処理装置を認証する第３の認証ステップと、第３の認証ステップの処理により他の情報処理装置が認証された場合、第２の記憶部に記憶されているデータを暗号化する第２の暗号化ステップと、第２の暗号化ステップの処理により暗号化されたデータを、ネットワークを介して他の情報処理装置に送信する送信ステップとを含むことを特徴とする。

第１の認証ステップの処理では、情報記憶媒体を認証した場合、情報記憶媒体との間で第１の暗号鍵を共有し、第１の暗号化ステップの処理では、第１の暗号鍵を用いてデータを暗号化し、第２の認証ステップの処理では、情報記憶媒体を認証した場合、情報記憶媒体との間で第２の暗号鍵を共有し、復号ステップの処理では、第２の暗号鍵を用いて暗号化されたデータを復号し、第３の認証ステップの処理では、他の情報処理装置を認証した場合、他の情報処理装置との間で第３の暗号鍵を共有し、第２の暗号化ステップの処理では、第３の暗号鍵を用いてデータを暗号化するものとすることができる。

第２の本発明においては、携帯型情報端末装置で、接続が確立された情報記憶媒体が認証された場合、記憶されているデータが暗号化されて情報記憶媒体に書き込まれ、情報処理装置で、接続が確立された情報記憶媒体が認証された場合、情報記憶媒体から暗号化されたデータが読み出されて復号され、接続が確立された他の情報処理装置が認証された場合、データが暗号化されてネットワークを介して他の情報処理装置に送信される。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】０１０６
【補正方法】変更
【補正の内容】
【０１０６】

【発明の効果】

本発明によれば、処理能力に制約のあるPDAなどの通信端末装置とサーバとの間において、低コストで、かつ、広帯域で秘匿性の高い通信路を確立することができる。