【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16年9月2日(2004.9.2)

【公開番号】特開2003-152714(P2003-152714A)
【公開日】平成15年5月23日(2003.5.23)
【出願番号】特願2001-350247(P2001-350247)
【国際特許分類第７版】
　Ｈ０４Ｌ　9/32
　Ｈ０４Ｌ　9/08
【ＦＩ】
　Ｈ０４Ｌ　9/00　６７５Ａ
　Ｈ０４Ｌ　9/00　６０１Ｃ

【手続補正書】
【提出日】平成15年8月19日(2003.8.19)
【手続補正１】
【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】
通信回線を介して接続されて互いに交信可能な配信用コンピュータおよび被配信用コンピュータからなるデータ通信システムにおいて、
前記配信用コンピュータおよび被配信用コンピュータが共通の事前共有鍵と一方向要約関数とを有し、
前記配信用コンピュータは、
送信データと前記事前共有鍵を引数として前記一方向要約関数にて要約値を生成する手段と、
前記送信データとともに前記要約値を送信する手段とを備え、
前記被配信用コンピュータは、
前記送信データとともに前記要約値を受信する手段と、
受信データと前記事前共有鍵を引数として前記一方向要約関数にて要約値を生成する手段と、
該要約値を前記配信用コンピュータから受信した要約値と比較し、送信データの改竄を検出する改竄検出手段と、
を備えたことを特徴とするデータ通信システム。
【請求項２】
通信回線を介して接続されて互いに交信可能な配信用コンピュータおよび被配信用コンピュータからなるデータ通信方法において、
データの配信に際し、被配信用コンピュータがデータを要求する毎に配信用コンピュータが当該データの識別データを生成し、
該識別データを受信した被配信用コンピュータが、この識別データに対応させて認識データを生成し、
被配信用コンピュータおよび配信用コンピュータにおいて、被配信用コンピュータと配信用コンピュータに予め備えた事前共有鍵と、前記識別データおよび認識データを引数として一方向関数による演算処理を施し、
この演算処理の結果により得られた関数値を含め、キー要求ファイルおよびキーファイルを生成することを特徴とするデータ通信方法。

【請求項３】
通信回線を介して接続されて互いに交信可能な配信用コンピュータおよび被配信用コンピュータからなるデータ通信システムに適用されるプログラムであって、
前記被配信用コンピュータからの要求に応じて、データベースに蓄積した一つまたは複数のデータを同被配信用コンピュータに送信する処理と、
前記配信用コンピュータにおいて、送信データと事前共有鍵を引数として一方向要約関数にて要約値を生成する処理、および送信データとともに前記要約値を送信する処理と、
前記被配信用コンピュータにおいて、送信データとともに前記要約値を受信する処理、および受信データと事前共有鍵を引数として前記一方向要約関数にて要約値を生成する処理、ならびに前記要約値を前記配信用コンピュータから受信した要約値と比較し、送信データの改竄を検出する改竄検出処理と、
を含むプログラムを記録したコンピュータ読み取り可能な記録媒体。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０００７
【補正方法】変更
【補正の内容】
【０００７】
【課題を解決するための手段】
本発明は、通信回線を介して接続されて互いに交信可能な配信用コンピュータおよび被配信用コンピュータからなるデータ通信システムにおいて、前記配信用コンピュータおよび被配信用コンピュータが共通の事前共有鍵と一方向要約関数とを有し、前記配信用コンピュータは、送信データと前記事前共有鍵を引数として前記一方向要約関数にて要約値を生成する手段と、前記送信データとともに前記要約値を送信する手段とを備え、前記被配信用コンピュータは、前記送信データとともに前記要約値を受信する手段と、受信データと前記事前共有鍵を引数として前記一方向要約関数にて要約値を生成する手段と、該要約値を前記配信用コンピュータから受信した要約値と比較し、送信データの改竄を検出する改竄検出手段と、を備えたデータ通信システムと、
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００８
【補正方法】変更
【補正の内容】
【０００８】
通信回線を介して接続されて互いに交信可能な配信用コンピュータおよび被配信用コンピュータからなるデータ通信方法において、データの配信の際し、被配信用コンピュータがデータを要求する毎に配信用コンピュータが当該データの識別データを生成し、該識別データを受信した被配信用コンピュータが、この識別データに対応させて認識データを生成し、被配信用コンピュータおよび配信用コンピュータにおいて、被配信用コンピュータと配信用コンピュータに予め備えた事前共有鍵と、前記識別データおよび認識データを引数として一方向関数による演算処理を施し、この演算処理の結果により得られた関数値を含め、キー要求ファイルおよびキーファイルを生成するデータ通信方法と、
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】変更
【補正の内容】
【０００９】
通信回線を介して接続されて互いに交信可能な配信用コンピュータおよび被配信用コンピュータからなるデータ通信システムに適用されるプログラムであって、前記被配信用コン

ピュータからの要求に応じて、データベースに蓄積した一つまたは複数のデータを同被配信用コンピュータに送信する処理と、前記配信用コンピュータにおいて、送信データと事前共有鍵を引数として一方向要約関数にて要約値を生成する処理、および送信データとともに前記要約値を送信する処理と、前記被配信用コンピュータにおいて、送信データとともに前記要約値を受信する処理、および受信データと事前共有鍵を引数として前記一方向要約関数にて要約値を生成する処理、ならびに前記要約値を前記配信用コンピュータから受信した要約値と比較し、送信データの改竄を検出する改竄検出処理と、を含むプログラムを記録したコンピュータ読み取り可能な記録媒体と、により上記課題を解決する。