

【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 19 年 6 月 14 日 (2007.6.14)

【公表番号】特表 2006-524950 (P2006-524950A)
 【公表日】平成 18 年 11 月 2 日 (2006.11.2)
 【年通号数】公開・登録公報 2006-043
 【出願番号】特願 2006-506888 (P2006-506888)
 【国際特許分類】

H 0 4 L 12/56 (2006.01)

H 0 4 L 29/10 (2006.01)

【F I】

H 0 4 L 12/56 3 0 0 A

H 0 4 L 12/56 B

H 0 4 L 13/00 3 0 9 A

【手続補正書】
 【提出日】平成 19 年 4 月 20 日 (2007.4.20)
 【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】

階層化通信モデルを用いてデータを送信する送信方法であって、

第 1 層において、第 1 エンティティを参照する第 1 アドレス参照を有する第 1 暗号法的保護された通信フラグメントを発生するステップと、

前記第 1 層の下第 2 層において、前記第 1 通信フラグメントに基づくと共に更に前記第 1 エンティティに関連する第 2 エンティティを参照する第 2 アドレス参照を有する第 2 通信フラグメントを発生するステップと、

前記第 2 通信フラグメントを有するデータを送信するステップと、
 を有する送信方法において、

当該送信方法が、

送信される前記データにおいて前記第 1 アドレス参照を少なくとも一部取り除くステップ

を更に有し、暗号法的保護が、前記第 1 アドレス参照が少なくとも一部取り除かれる前に、前記第 1 通信フラグメントに関して提供されることを特徴とする送信方法。

【請求項 2】

請求項 1 に記載の送信方法であって、暗号法的保護が、前記通信モデルにおける 1 つの層においてのみ提供される送信方法。

【請求項 3】

請求項 2 に記載の伝送方法であって、前記 1 つの層が、前記メッセージが開始される層に等しい送信方法。

【請求項 4】

請求項 1 に記載の送信方法であって、前記第 1 アドレス参照が、前記第 2 アドレス参照を参照する情報フィールドによって置き換えられる送信方法。

【請求項 5】

階層化通信モデルを用いてデータを受信する受信方法であって、

第 1 エンティティに関連する第 2 エンティティを参照する第 2 アドレス参照を有すると

共に、

前記第 1 エンティティに対する第 1 アドレス参照を有する第 1 暗号法的保護された通信フラグメントに基づく

第 2 通信フラグメントを有するデータを受信するステップと、

前記第 2 通信フラグメントから前記第 1 通信フラグメントを取得するステップと、

を有する受信方法において、

前記第 1 アドレス参照が、受信された前記データにおいて少なくとも一部省かれ、

前記受信方法が、前記第 1 通信フラグメントを取得する際に前記第 1 アドレス参照を修復するステップを更に有し、前記第 1 通信フラグメントの暗号法的保護が、前記第 1 アドレス参照が取得された後に確認される

ことを特徴とする受信方法。

【請求項 6】

請求項 5 に記載の受信方法であって、暗号法的保護が、前記通信モデルにおける 1 つの層のみににおいて提供される受信方法。

【請求項 7】

請求項 6 に記載の受信方法であって、前記 1 つの層が、前記メッセージが開始される層に等しい受信方法。

【請求項 8】

請求項 5 に記載の受信方法であって、当該受信方法が、受信された前記データにおける情報フィールドを用いて前記第 1 アドレス参照を取得する受信方法であって、前記情報フィールドが、前記第 1 アドレス参照を置き換えると共に前記第 2 アドレス参照を参照する受信方法。

【請求項 9】

階層化通信モデルを用いて通信するシステムであって、

第 1 層において、第 1 エンティティを参照する第 1 アドレス参照を有する第 1 暗号法的保護された通信フラグメントを発生するように構成されると共に、

前記第 1 層の下第 2 層において、前記第 1 通信フラグメントに基づくと共に前記第 1 エンティティに関連する第 2 エンティティを参照する第 2 アドレス参照を更に有する第 2 通信フラグメントを発生するように構成される

送信手段と、

前記第 2 通信フラグメントを有するデータを送信するように構成される通信手段と、

前記第 2 通信フラグメントを有するデータを受信するように構成されると共に、

前記第 2 通信フラグメントから前記第 1 通信フラグメントを取得するように更に構成される

受信手段と

を有するシステムにおいて、

前記送信手段が、前記送信データから前記第 1 アドレス参照を少なくとも一部省くように構成され、

前記受信手段が、前記受信データから前記第 1 通信フラグメントを取得する際に前記第 1 アドレス参照を修復するように構成される

ことを特徴とするシステム。

【請求項 10】

階層化通信モデルを用いてデータを送信する送信器装置であって、

第 1 層において、第 1 エンティティを参照する第 1 アドレス参照を有する第 1 暗号法的保護された通信フラグメントを発生するように構成され、

更に、前記第 1 層の下第 2 層において、前記第 1 通信フラグメントに基づくと共に、前記第 1 エンティティに関連する第 2 エンティティを参照する第 2 アドレス参照を更に有する、第 2 通信フラグメントを発生するように構成され、

更に、前記第 2 通信フラグメントを有するデータを送信するように構成される

送信器装置において、

当該送信器装置が、送信される前記データにおける前記第 1 アドレス参照を少なくとも一部取り除くように更に構成されることを特徴とする送信器装置。

【請求項 1 1】

階層化通信モデルを用いてデータを受信する受信器装置であって、

第 1 エンティティに関連する第 2 エンティティを参照する第 2 アドレス参照を有すると共に

前記第 1 エンティティに対する第 1 アドレス参照を有する第 1 暗号法的保護された通信フラグメントに基づく

第 2 通信フラグメントを有するデータを受信するように構成され、

更に、前記第 2 通信フラグメントから前記第 1 通信フラグメントを取得するように構成される

受信器装置において、

前記第 1 アドレス参照が、受信される前記データにおいて少なくとも一部省かれ、

当該受信器装置が、前記第 1 通信フラグメントを取得する際に、前記第 1 アドレス参照を修復するように更に構成されることを特徴とする受信器装置。

【請求項 1 2】

階層化通信モデルを用いて通信を実行する送信器計算機プログラムであって、当該送信器計算機プログラムが、

第 1 層において、第 1 エンティティを参照する第 1 アドレス参照を有する第 1 暗号法的保護された通信フラグメントを発生するように構成され、

更に、前記第 1 層の下第 2 層において、前記第 1 通信フラグメントに基づくと共に、前記第 1 エンティティに関連する第 2 エンティティを参照する第 2 アドレス参照を更に有する第 2 通信通信フラグメントを発生するように構成され、

更に、前記第 2 通信フラグメントを有するデータを送信するように構成される

送信器計算機プログラムにおいて、

当該送信器計算機プログラムが、前記送信データにおいて前記第 1 アドレス参照を省くように更に構成される

ことを特徴とする送信器計算機プログラム。

【請求項 1 3】

階層化通信モデルを用いて通信を実行する受信器計算機プログラムであって、

第 1 通信エンティティに関連する第 2 エンティティを参照する第 2 アドレス参照を有すると共に、

前記第 1 エンティティに対する第 1 アドレス参照を有する第 1 暗号法的保護された通信フラグメントに基づく

第 2 通信フラグメントを有するデータを受信するように構成され、

更に、前記第 2 通信フラグメントから前記第 1 通信フラグメントを取得するように構成され、ここで、

第 1 層においては、第 1 エンティティを参照する第 1 アドレス参照を有する第 1 通信フラグメントが発生され、

前記第 1 層の下第 2 層においては、前記第 1 エンティティに関連する第 2 エンティティを参照する第 2 アドレス参照を有すると共に前記第 1 通信フラグメントに基づく第 2 通信フラグメントが発生される、

受信器計算機プログラムにおいて、

前記第 1 アドレス参照が、前記受信されたデータにおいて少なくとも一部省かれ、

当該受信器計算機プログラムが、前記第 1 通信フラグメントを取得する際に、前記第 1 アドレス参照を修復するように更に構成される

ことを特徴とする受信器計算機プログラム。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0001

【補正方法】変更

【補正の内容】

【0001】

本発明は、階層化通信モデルを用いてデータを送信する送信方法であって、第1エンティティを参照する第1アドレス参照を有する第1暗号法的保護された通信フラグメントを第1層に発生するステップと、第1通信フラグメントに基づくと共に更に前記第1エンティティに関連する第2エンティティを参照する第2アドレス参照を有する第2通信フラグメントを前記第1層の下第2層に発生するステップと、前記第2通信フラグメントを有する送信データを送信するステップとを有する送信方法に関する。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0002

【補正方法】変更

【補正の内容】

【0002】

また本発明は、階層化通信モデルを用いてデータを受信する受信方法であって、第1エンティティに関連する第2エンティティを参照する第2アドレス参照を有し、且つ前記第1エンティティに対する第1アドレス参照を有する第1暗号法的保護された通信フラグメントに基づく第2通信フラグメントを有するデータを受信するステップと、前記第2通信フラグメントから前記第1通信フラグメントを取得するステップとを有するような受信方法にも関する。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0003

【補正方法】変更

【補正の内容】

【0003】

更に本発明は、階層化通信モデルを用いた通信に関するシステムであって、第1エンティティを参照する第1アドレス参照を有する第1暗号法的保護された通信フラグメントを第1層に発生するように構成され、前記第1通信フラグメントに基づき第2通信フラグメントを前記第1層の下第2層において発生するように更に構成され、前記第1エンティティに関連する第2エンティティを参照する第2アドレス参照を更に有する送信器手段と、前記第2通信フラグメントを有するデータを送信するように構成される通信手段と、前記第2通信フラグメントを有するデータを受信するように構成されると共に更に前記第2通信フラグメントから前記第1通信フラグメントを取得するように構成される受信手段とを有するシステムに関する。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0004

【補正方法】変更

【補正の内容】

【0004】

更に本発明は、階層化通信モデルを用いてデータを送信する送信器装置であって、第1エンティティを参照する第1アドレス参照を有する第1暗号法的保護された通信フラグメントを第1層において発生するように構成され、更に、前記第1通信フラグメントに基づく第2通信フラグメントを前記第1層の下第2層において発生するように構成され、更に、前記第1エンティティに関連する第2エンティティを参照する第2アドレス参照を有し、更に、前記第2通信フラグメントを有するデータを送信するように構成される送信器

装置に関する。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0005

【補正方法】変更

【補正の内容】

【0005】

また本発明は、階層化通信モデルを用いてデータを受信する受信器装置であって、当該受信器装置が、第2通信フラグメントを有するデータを受信するように構成され、前記第2通信フラグメントが、第1エンティティに関連する第2エンティティを参照する第2アドレス参照を有し、前記第1エンティティに対する第1アドレス参照を有する第1暗号法的保護された通信フラグメントに基づき、更に前記第2通信フラグメントから前記第1通信フラグメントを取得するように構成されるような受信器装置にも関する。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0006

【補正方法】変更

【補正の内容】

【0006】

更に本発明は、階層化通信モデルに従い発生されるデータを担持する信号であって、前記データが、第1エンティティを参照する第1アドレス参照を有する第1暗号法的保護された通信フラグメントが発生される第1層と、前記第1通信フラグメントに基づく前記第1エンティティに関連する第2エンティティを参照する第2アドレス参照を有する第2通信フラグメントが発生される前記第1層の下の第2層とを有する階層化通信モデルに従い発生されるような信号に関する。

【手続補正 8】

【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】

更に本発明は、階層化通信モデルを用いて通信を実行する送信器計算機プログラムであって、送信器計算機プログラムが、第1エンティティを参照する第1アドレス参照を有する第1暗号法的保護された通信フラグメントを第1層において発生するように構成され、更に、前記第1通信フラグメントに基づく第2通信フラグメントを第1層の下の第2層において発生するように構成され、更に、前記第1エンティティに関連する第2エンティティを参照する第2アドレス参照を有し、更に、前記第2通信フラグメントを有するデータを送信するように構成される送信器計算機プログラムに関する。

【手続補正 9】

【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】

また本発明は、階層化通信モデルを用いて通信を実行する受信器計算機プログラムであって、当該受信器計算機プログラムが、第1エンティティに関連する第2エンティティを参照する第2アドレス参照を有すると共に前記第1エンティティに対する第1アドレス参照を有する第1暗号法的保護された通信フラグメントに基づく第2通信フラグメントを有するデータを受信するように構成され、更に、前記第2通信フラグメントから前記第1通信フラグメントを取得するように構成され、ここで、第1層においては、第1エンティテ

ィを参照する第1アドレス参照を有する第1通信フラグメントが発生され、前記第1層の下第2層においては、前記第1エンティティに関連する第2エンティティを参照する第2アドレス参照を有すると共に前記第1通信フラグメントに基づく第2通信フラグメントが発生される受信器計算機プログラムにも関する。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正の内容】

【0010】

本発明の目的は、物理的フレームのサイズが低減される一方で、包含される情報がほぼ維持される送信方法、及びその暗号法的保護を提供することである。

【手続補正11】

【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】

この目的は、送信されるデータにおける第1アドレス参照を少なくとも一部取り除くステップを更に有し、且つ暗号法的保護が、前記第1アドレス参照が少なくとも一部取り除かれる前に、前記第1通信フラグメントに関して提供されることを特徴とする本発明による送信方法によって実現される。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正の内容】

【0012】

この方法は、第1アドレス参照が省かれる第1通信フラグメントの保護を扱う。フレームを暗号法的に保護することを所望する特定の層は、各々のフレームに関してメッセージ完全性符号(MIC)が発生し得る。任意のストリングにおけるMICは、例えば、CBC-MACモードにおけるブロック暗号(Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, 353ページを参照)を用いて発生され得る。フレーム保護の場合、CBC-MACへの入力、保護されるべきフレームになり、可能であればフレームの長さを示す数を接頭子として付けられる。MICが決定された後、MICは、フレームが送信される前にフレームペイロードに加えられる。

【手続補正13】

【補正対象書類名】明細書

【補正対象項目名】0015

【補正方法】変更

【補正の内容】

【0015】

本発明による方法の一実施例は、請求項2に記載される。この実施例は、通信層における1つのレベルにおいてのみ暗号法的保護が加えられ、これによりオーバーヘッドが低減されるという有利な点を有する。

【手続補正14】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

【補正の内容】

【0016】

本発明による方法の一実施例は、請求項3に記載される。この実施例は、各々メッセージが、1つのフレームに納まるのに通常十分短い（すなわち、各々のレベルにおけるメッセージが最大許容ペイロードより小さい）ような実施例において、演算を開始のレベルである可能最高位レベルにおいて実行することによって、MICを加えるオーバーヘッドが最小化されるという有利な点を有する。

【手続補正15】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】変更

【補正の内容】

【0017】

本発明による方法の一実施例は、請求項4に記載される。省かれるべき複写情報は、省かれたデータが見つけれられ得る場所を示す、より短いフィールドによって置き換えされる。

【手続補正16】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正の内容】

【0018】

本発明の更なる目的は、物理的フレームのサイズが低減される一方で、包含される情報をほぼ維持する受信方法、及びその暗号法的保護を提供することである。

【手続補正17】

【補正対象書類名】明細書

【補正対象項目名】0019

【補正方法】変更

【補正の内容】

【0019】

この目的は、第1アドレス参照が、受信されたデータにおいて少なくとも一部省かれることを特徴とする本発明による受信方法であって、当該受信方法が、更に、第1通信フラグメントを取得する際に第1アドレス参照を修復するステップを有し、且つ前記第1通信フラグメントの暗号法的保護が、前記第1アドレス参照が取得された後に確認される、本発明による受信方法によって実現される。

【手続補正18】

【補正対象書類名】明細書

【補正対象項目名】0020

【補正方法】変更

【補正の内容】

【0020】

本発明による受信方法の更なる実施例は、請求項6、7及び8に記載される。これらの実施例は、上記の実施例に補足するものである。