(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5890586号
(P5890586)

(45)発行日　平成28年3月22日(2016.3.22)　(24)登録日　平成28年2月26日(2016.2.26)

(51)Int.Cl.			F I		
H04L	9/14	(2006.01)	H04L	9/00	641
G09C	1/00	(2006.01)	G09C	1/00	660D
H04L	29/06	(2006.01)	H04L	13/00	305C

請求項の数 10　(全 18 頁)

(21)出願番号	特願2015-511475 (P2015-511475)
(86)(22)出願日	平成25年3月28日 (2013.3.28)
(65)公表番号	特表2015-523766 (P2015-523766A)
(43)公表日	平成27年8月13日 (2015.8.13)
(86)国際出願番号	PCT/US2013/034212
(87)国際公開番号	WO2013/169409
(87)国際公開日	平成25年11月14日 (2013.11.14)
審査請求日	平成26年12月17日 (2014.12.17)
(31)優先権主張番号	13/466,251
(32)優先日	平成24年5月8日 (2012.5.8)
(33)優先権主張国	米国(US)

(73)特許権者　391030332
アルカテル－ルーセント
フランス国、９２１００・ブローニュ－ビヤンクール、ルート・ドゥ・ラ・レーヌ・１４８／１５２
(74)代理人　100094112
弁理士　岡部　讓
(74)代理人　100106183
弁理士　吉澤　弘司
(74)代理人　100170601
弁理士　川崎　孝
(74)代理人　100187964
弁理士　新井　剛

最終頁に続く

(54)【発明の名称】クラウド・ネットワークにおける接続高速化のための方法および装置

(57)【特許請求の範囲】

【請求項１】

高速化接続システムでターゲット・ファイルの暗号化を提供するための装置であって、

データ記憶装置と

前記データ記憶装置に通信可能に接続されたプロセッサであって、

第１のクライアントからの要求に応じて、前記ターゲット・ファイルを少なくとも１つの第１の静的ファイル・チャンクおよび少なくとも１つの第１の動的ファイル・チャンクに分割し、

第２のクライアントからの要求に応じて、前記ターゲット・ファイルを少なくとも１つの第２の静的ファイル・チャンクおよび少なくとも１つの第２の動的ファイル・チャンクに分割し、

第１の暗号化方式に基づいて、前記少なくとも１つの第１の静的ファイル・チャンクの第１の暗号化された静的ファイル・チャンクを作成し、

第２の暗号化方式に基づいて、前記少なくとも１つの第１の動的ファイル・チャンクの第１の暗号化された動的ファイル・チャンクを作成し、

第１の暗号化方式に基づいて、前記少なくとも１つの第２の静的ファイル・チャンクの第２の暗号化された静的ファイル・チャンクを作成し、

第２の暗号化方式に基づいて、前記少なくとも１つの第２の動的ファイル・チャンクの第２の暗号化された動的ファイル・チャンクを作成する、

ように構成されているプロセッサと

を含み、
前記第１のクライアントと前記第２のクライアントは異なり、
前記第１の暗号化方式と前記第２の暗号化方式は異なり、
前記第１の暗号化された静的ファイル・チャンクと前記第２の暗号化された静的ファイル・チャンクは同じである
装置。
【請求項２】
前記暗号化された静的ファイル・チャンクの作成は、
第３の暗号化方式を使用して、前記第１の暗号化された静的ファイル・チャンクに対する復号鍵である第１の静的な暗号鍵を暗号化する、
ように前記プロセッサをさらに構成することを含む請求項１に記載の装置。
【請求項３】
前記少なくとも１つの第１の静的ファイル・チャンクへの前記ターゲット・ファイルの分割は、
前記少なくとも１つの第１の静的ファイル・チャンクが複数のクライアントに共通するデータを含むことを判定する
ようにプロセッサを構成することを含む請求項１に記載の装置。
【請求項４】
前記少なくとも１つの第１の動的ファイル・チャンクへの前記ターゲット・ファイルの分割は、
前記少なくとも１つの第１の動的ファイル・チャンクが、
個人データ、
ＨＴＭＬ形式の情報、および
一時データ
の少なくとも１つを含むことを判定する
ように前記プロセッサを構成することを含む請求項１に記載の装置。
【請求項５】
前記プロセッサは、
前記第１の静的ファイル・チャンクが静的データであることを示すメッセージを作成する、
ようにさらに構成されている請求項１に記載の装置。
【請求項６】
高速化接続システムでターゲット・ファイルの暗号化を提供するための方法であって、
データ記憶装置に通信可能に接続されたプロセッサで、第１のクライアントからの要求に応じて、前記ターゲット・ファイルを少なくとも１つの第１の静的ファイル・チャンクおよび少なくとも１つの第１の動的ファイル・チャンクに分割するステップと、
前記データ記憶装置と協働する前記プロセッサによって、第２のクライアントからの要求に応じて、前記ターゲット・ファイルを少なくとも１つの第２の静的ファイル・チャンクおよび少なくとも１つの第２の動的ファイル・チャンクに分割するステップと、
前記データ記憶装置と協働する前記プロセッサによって、第１の暗号化方式に基づいて、前記少なくとも１つの第１の静的ファイル・チャンクの第１の暗号化された静的ファイル・チャンクを作成するステップと、
前記データ記憶装置と協働する前記プロセッサによって、第２の暗号化方式に基づいて、前記少なくとも１つの第１の動的ファイル・チャンクの第１の暗号化された動的ファイル・チャンクを作成するステップと、
前記データ記憶装置と協働する前記プロセッサによって、第１の暗号化方式に基づいて、前記少なくとも１つの第２の静的ファイル・チャンクの第２の暗号化された静的ファイル・チャンクを作成するステップと
前記データ記憶装置と協働する前記プロセッサによって、第２の暗号化方式に基づいて、前記少なくとも１つの第２の動的ファイル・チャンクの第２の暗号化された動的ファイ

ル・チャンクを作成するステップと
を含み、
前記第１のクライアントと前記第２のクライアントは異なり、
前記第１の暗号化方式と前記第２の暗号化方式は異なり、
前記第１の暗号化された静的ファイル・チャンクと前記第２の暗号化された静的ファイル・チャンクは同じである
方法。
【請求項７】
前記データ記憶装置と協働する前記プロセッサによって、前記第１のクライアントに前記第１の暗号化された静的ファイル・チャンクを送信するステップと、
前記データ記憶装置と協働する前記プロセッサによって、前記第１のクライアントに前記第１の暗号化された動的ファイル・チャンクを送信するステップと、
前記データ記憶装置と協働する前記プロセッサによって、前記第２のクライアントに前記第２の暗号化された静的ファイル・チャンクおよび前記第２の暗号化された動的ファイル・チャンクを送信するステップと
前記データ記憶装置と協働する前記プロセッサによって、前記第２のクライアントに前記第２の暗号化された静的ファイル・チャンクおよび前記第２の暗号化された動的ファイル・チャンクを送信するステップと
をさらに含む請求項６に記載の方法。
【請求項８】
前記第１の暗号化された静的ファイル・チャンクを作成するステップは、
第３の暗号化方式を使用して、前記第１の暗号化された静的ファイル・チャンクに対する復号鍵である第１の静的な暗号鍵を暗号化するステップ
を含む請求項６に記載の方法。
【請求項９】
前記データ記憶装置と協働する前記プロセッサによって、前記第１の静的ファイル・チャンクが静的データであることを示すメッセージを作成するステップと、
前記データ記憶装置と協働する前記プロセッサによって、高速化ミドルボックスに前記メッセージを送信するステップと
をさらに含み、
暗号化された動的ファイル・チャンクはＨＴＴＰＳを使用する請求項６に記載の方法。
【請求項１０】
前記第１の暗号化された静的ファイル・チャンクを作成し、前記第１の暗号化された動的ファイル・チャンクを作成するステップは、前記アプリケーション・レイヤで行われる請求項６に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的に、クラウド・ネットワークにおいて高速化接続を提供するための方法および装置に関する。
【背景技術】
【０００２】
本項では、本発明についてより深い理解を促進するために役に立つ可能性がある態様を紹介する。したがって、本項の記述は、この観点から読むべきものであり、従来技術ではどのようなものであったか、または従来技術ではどのようなものでなかったかに関する認識として理解するべきではない。
【０００３】
一部の知られている高速化接続システムでは、ＷＡＮ高速化ミドルボックスが、以前に受信されたデータを記憶し、データ重複排除を通じて、アプリケーション遅延を減らして帯域幅を節約するために、新しく受信されたデータのうち繰り返されるバイト・シーケン

スを識別子に置き換える。

【０００４】

知られている一部のアプリケーション・サーバでは、暗号化されたデータがクラウド・サーバからクライアントに配布される。これらの知られているシステムの一部では、暗号化された接続は、異なるユーザに対して異なる鍵を使う（すなわち、ユーザごとの暗号化を行う）ため、同一の送信データに対する異なる暗号文が用いられることとなる。

【発明の概要】

【課題を解決するための手段】

【０００５】

様々な実施形態において、ユーザごとに暗号化されたデータを含むデータの送信をサポートするクラウド・ネットワークにおいて、高速化され、暗号化された接続を提供する方法および装置を提供する。アプリケーション・サーバからの暗号化されたデータの送信は、コンテンツ自体から鍵を取得する第１の暗号化方式を使用して静的データを暗号化し、第２の暗号化方式を使用して個別化されたユーザ・データを用いる動的ウェブサイト・コンテンツなどの動的データを暗号化する、暗号化方式を使用する。有利なことに、この暗号化方式は、従来の高速化ミドルボックスが暗号化された静的データの重複を排除することを可能にする。

【０００６】

一実施形態では、高速化接続システムでターゲット・ファイルの暗号化を提供するための装置が提供される。装置は、データ記憶装置、およびデータ記憶装置に通信可能に接続されたプロセッサを含む。プロセッサは、第１のクライアントからの要求に応じて、ターゲット・ファイルを少なくとも１つの第１の静的ファイル・チャンクおよび少なくとも１つの第１の動的ファイル・チャンクへと分割し、第２のクライアントからの要求に応じて、ターゲット・ファイルを少なくとも１つの第２の静的ファイル・チャンクおよび少なくとも１つの第２の動的ファイル・チャンクに分割し、第１の暗号化方式に基づいて、少なくとも１つの第１の静的ファイル・チャンクの第１の暗号化された静的ファイル・チャンクを作成し、第２の暗号化方式に基づいて、少なくとも１つの第１の動的ファイル・チャンクの第１の暗号化された動的ファイル・チャンクを作成し、第１の暗号化方式に基づいて、少なくとも１つの第２の静的ファイル・チャンクの第２の暗号化された静的ファイル・チャンクを作成し、第２の暗号化方式に基づいて、少なくとも１つの第２の動的ファイル・チャンクの第２の暗号化された動的ファイル・チャンクを作成するようにプログラムされている。装置において、第１のクライアントと第２のクライアントは異なり、第１の暗号化方式と第２の暗号化方式は異なり、第１の暗号化された静的ファイル・チャンクと第２の暗号化された静的ファイル・チャンクは同じである。

【０００７】

上記の実施形態の一部では、第１の暗号化方式は収束暗号化である。

【０００８】

上記の実施形態の一部では、第２の暗号化方式は対称鍵暗号化である。

【０００９】

上記の実施形態の一部では、暗号化された静的ファイル・チャンクの作成は、第３の暗号化方式を使用して、第１の静的な暗号鍵は、第１の暗号化された静的ファイル・チャンクに対する復号鍵である第１の静的な暗号鍵を暗号化するようにプロセッサをさらにプログラムすることを含む。

【００１０】

上記の実施形態の一部では、第２の暗号化方式は、第３の暗号化方式と同じである。

【００１１】

上記の実施形態の一部では、少なくとも１つの第１の静的ファイル・チャンクへのターゲット・ファイルの分割は、少なくとも１つの第１の静的ファイル・チャンクが複数のクライアントに共通するデータを含むことを判定するようにプロセッサをプログラムすることを含む。

【００１２】
上記の実施形態の一部では、少なくとも１つの第１の動的ファイル・チャンクへのターゲット・ファイルの分割は、少なくとも１つの第１の動的ファイル・チャンクが、個人データ、ＨＴＭＬ形式の情報、または一時データを含むことを判定するようにプロセッサをプログラムすることを含む。
【００１３】
上記の実施形態の一部では、プロセッサは、第１の静的ファイル・チャンクが静的データであることを示すメッセージを作成するようさらにプログラムされる。
【００１４】
上記の実施形態の一部では、第１の暗号化された静的ファイル・チャンクの作成および第１の暗号化された動的ファイル・チャンクの作成は、アプリケーション・レイヤで行われる。
【００１５】
第２の実施形態では、高速化接続システムでターゲット・ファイルを配布するためのシステムが提供される。システムは、第１のクライアントおよび第２のクライアントを含む複数のクライアント、少なくとも第１のクライアントおよび第２のクライアントに接続された少なくとも１つの高速化ミドルボックス、ならびに高速化ミドルボックスおよび少なくとも第１のクライアントおよび第２のクライアントに接続されたアプリケーション・サーバを含む。アプリケーション・サーバは、第１のクライアントからの要求に応じて、ターゲット・ファイルを少なくとも１つの第１の静的ファイル・チャンクおよび少なくとも１つの第１の動的ファイル・チャンクに分割し、第２のクライアントからの要求に応じて、ターゲット・ファイルを少なくとも１つの第２の静的ファイル・チャンクおよび少なくとも１つの第２の動的ファイル・チャンクに分割し、第１の暗号化方式に基づいて、少なくとも１つの第１の静的ファイル・チャンクの第１の暗号化された静的ファイル・チャンクを作成し、第２の暗号化方式に基づいて、少なくとも１つの第１の動的ファイル・チャンクの第１の暗号化された動的ファイル・チャンクを作成し、第１の暗号化方式に基づいて、少なくとも１つの第２の静的ファイル・チャンクの第２の暗号化された静的ファイル・チャンクを作成し、第２の暗号化方式に基づいて、少なくとも１つの第２の動的ファイル・チャンクの第２の暗号化された動的ファイル・チャンクを作成し、高速化ミドルボックスを介して、第１のクライアントに第１の暗号化された静的ファイル・チャンクおよび第１の暗号化された動的ファイル・チャンクを送信し、高速化ミドルボックスを介して、第２のクライアントに第２の暗号化された静的ファイル・チャンクおよび第２の暗号化された動的ファイル・チャンクを送信するようにプログラムされている。高速化ミドルボックスは、高速化方式を第１の暗号化された静的ファイル・チャンクおよび第２の暗号化された静的ファイル・チャンクに適用するようにプログラムされている。第１のクライアントは、第１の暗号化された静的ファイル・チャンクおよび第１の暗号化された動的ファイル・チャンクに基づいて、ターゲット・ファイルを取得するようにプログラムされている。第２のクライアントは、第２の暗号化された静的ファイル・チャンクおよび第２の暗号化された動的ファイル・チャンクに基づいて、ターゲット・ファイルを取得するようにプログラムされている。システムでは、第１のクライアントと第２のクライアントは異なり、第１の暗号化方式と第２の暗号化方式は異なり、第１の暗号化された静的ファイル・チャンクと第２の暗号化された静的ファイル・チャンクは同じである。
【００１６】
上記の実施形態の一部では、アプリケーション・サーバは、第２の暗号化方式を使用してメッセージを暗号化し、メッセージは、第１の静的ファイル・チャンクが静的データであることを示し、高速化ミドルボックスにメッセージを送信するようにさらにプログラムされている。システムでは、高速化ミドルボックスは、メッセージに基づいて高速化方式を適用する。
【００１７】
第３の実施形態では、高速化接続システムでターゲット・ファイルの暗号化を提供する

ための方法が提供される。方法は、第１のクライアントからの要求に応じて、ターゲット・ファイルを少なくとも１つの第１の静的ファイル・チャンクおよび少なくとも１つの第１の動的ファイル・チャンクへと分割するステップと、第２のクライアントからの要求に応じて、ターゲット・ファイルを少なくとも１つの第２の静的ファイル・チャンクおよび少なくとも１つの第２の動的ファイル・チャンクに分割するステップと、第１の暗号化方式に基づいて、少なくとも１つの第１の静的ファイル・チャンクの第１の暗号化された静的ファイル・チャンクを作成するステップと、第２の暗号化方式に基づいて、少なくとも１つの第１の動的ファイル・チャンクの第１の暗号化された動的ファイル・チャンクを作成するステップと、第１の暗号化方式に基づいて、少なくとも１つの第２の静的ファイル・チャンクの第２の暗号化された静的ファイル・チャンクを作成するステップと、第２の暗号化方式に基づいて、少なくとも１つの第２の動的ファイル・チャンクの第２の暗号化された動的ファイル・チャンクを作成するステップとを含む。方法では、第１のクライアントと第２のクライアントは異なり、第１の暗号化方式と第２の暗号化方式は異なり、第１の暗号化された静的ファイル・チャンクと第２の暗号化された静的ファイル・チャンクは同じである。

【００１８】

上記の実施形態の一部では、方法は、第１のクライアントに第１の暗号化された静的ファイル・チャンクを送信するステップと、第１のクライアントに第１の暗号化された動的ファイル・チャンクを送信するステップと、第２のクライアントに第２の暗号化された静的ファイル・チャンクおよび第２の暗号化された動的ファイル・チャンクを送信するステップと、第２のクライアントに第２の暗号化された静的ファイル・チャンクおよび第２の暗号化された動的ファイル・チャンクを送信するステップとをさらに含む。

【００１９】

上記の実施形態の一部では、第１の暗号化方式は収束暗号化である。

【００２０】

上記の実施形態の一部では、第２の暗号化方式は対称鍵暗号化である。

【００２１】

上記の実施形態の一部では、暗号化された静的なファイル・チャンクの作成は、第３の暗号化方式を使用して、第１の暗号化された静的ファイル・チャンクに対する復号鍵である第１の静的な暗号鍵を暗号化するステップを含む。

【００２２】

上記の実施形態の一部では、方法は、第１の静的ファイル・チャンクが静的データであることを示すメッセージを作成するステップと、高速化ミドルボックスにメッセージを送信するステップとをさらに含む。

【００２３】

上記の実施形態の一部では、第１の暗号化された動的ファイル・チャンクを含むパケットはメッセージを含む。

【００２４】

上記の実施形態の一部では、第１の暗号化された動的ファイル・チャンクを送信するステップは、ＨＴＴＰＳを使用する。

【００２５】

上記の実施形態の一部では、第１の暗号化された静的ファイル・チャンクを作成し、第１の暗号化された動的ファイル・チャンクを作成するステップは、アプリケーション・レイヤで行われる。

【００２６】

添付の図面において、様々な実施形態について説明する。

【図面の簡単な説明】

【００２７】

【図１】クラウド・ネットワークに高速化接続システム１００の実施形態を含むクラウド・ネットワークを示す図である。

【図２】図１の高速化接続システム１００が、ユーザごとに暗号化されたデータを含むファイルの送信を提供するための方法２００の実施形態を示すフローチャートである。
【図３】図２のステップ２２０に示すように、アプリケーション・サーバがデータを暗号化するための方法３００の実施形態を示すフローチャートである。
【図４】図２のステップ２４０に示すように、１対の高速化ミドルボックスが高速化方式を提供するための方法４００の実施形態を示すフローチャートである。
【図５】図１のアプリケーション・サーバ１２０または図１の高速化ミドルボックス１５０の１つなど、様々な装置５００の実施形態を概略的に示す図である。
【発明を実施するための形態】
【００２８】
理解を容易にするために、本質的に同じもしくは類似の構造、または本質的に同じもしくは類似の機能を持つ要素を示すために、同一の参照番号が使用されている。
【００２９】
記述および図面は、単に本発明の原理を示すものである。当業者であれば、本明細書に明示的に記述して示していないが、本発明の原理を具体化し、その範囲に含まれる様々な配置を考案できることを理解されるだろう。さらに、本明細書に詳述したすべての例は、原則として、読者が本発明の原理、およびその技術を推進する発明者（ら）によって提供された概念を理解するのを支援するために、教育のみを目的とすることを明確に意図するものであり、そのような具体的に詳述された例および条件に限定しないものとして解釈するべきである。さらに、本明細書に使用する「または（ｏｒ）」という用語は、そうでないことが明記されていない限り（たとえば、「さもなければ（ｏｒ　ｅｌｓｅ）」または「別の方法では（ｉｎ　ｔｈｅ　ａｌｔｅｒｎａｔｉｖｅ）」など）、非排他的な「または（ｏｒ）」を示している。また、本明細書に記述した様々な実施形態は、必ずしも相互排他的ではなく、一部の実施形態は、新しい実施形態を形成するために、１つまたは複数の他の実施形態と組み合わせることができる。
【００３０】
様々な実施形態において、ユーザごとに暗号化されたデータを含むファイルの送信をサポートするクラウド・ネットワークにおいて、高速化され、暗号化された接続を提供する方法および装置が提供される。アプリケーション・サーバからの暗号化されたファイルの送信は、コンテンツ自体から鍵を取得する第１の暗号化方式を使用して静的データを暗号化し、第２の暗号化方式を使用して、個別化されたユーザ・データを用いる動的なウェブサイト・コンテンツなど、動的データを暗号化する暗号化方式を使用する。
【００３１】
図１は、クラウド・ネットワークに高速化接続システム１００の実施形態を含むクラウド・ネットワークを示す図である。高速化接続システム１００は、通信路を通じて、１つまたは複数のクライアント１８０－ａ～１８０－ｃ（まとめて、クライアント１８０）にデータを配布するアプリケーション・サーバ１２０を含む。通信路は、アプリケーション通信チャネル１２５、高速化ミドルボックス１５０－ａおよび１５０－ｂ（まとめて、高速化ミドルボックス１５０）、高速化ミドルボックス通信チャネル１５５－ａおよび１５５－ｂ（まとめて、高速化ミドルボックス通信チャネル１５５）、ネットワーク１３０、ならびにクライアント通信チャネル１８５－ａ～１８５－ｃ（まとめて、クライアント通信チャネル１８５）の１つを含む。
【００３２】
アプリケーション・サーバ１２０は、アプリケーション・サーバ通信チャネル１２５を通じてクライアント１８０の１つまたは複数にファイルを送信できる任意の装置の場合がある。特に、アプリケーション・サーバは、第１の暗号化方式を使用して、複数のクライアントに共通するデータなど、静的ファイル・チャンクを暗号化する暗号化方式を使用して、暗号化ファイルを送信し、第２の暗号化方式を使用して、個別化されたユーザ・データを用いる動的なウェブサイトのコンテンツなど、動的ファイル・チャンクを暗号化する。

【００３３】
本明細書で使用する「ファイル」および「チャンク」という用語は、任意のアプリケーション・コンテンツを意味するものであり、アプリケーション・サーバ通信チャネル１２５を通じて送信または受信できる任意のコンテンツを含むものとして広く理解するべきである。たとえば、ファイルおよびファイル・チャンクは、従来のファイル、パケット、パケットのストリーム、デジタル文書、ビデオまたは映像のコンテンツ、ファイル・ブロック、データ・オブジェクト、前述のものの一部などを含むことができる。
【００３４】
通信チャネル１２５、１５５、および１８５は、ワイヤレス通信（たとえばＬＴＥ、ＧＳＭ、ＣＤＭＡ、ブルートゥース）、フェムトセル通信（たとえばＷｉＦｉ）、パケット・ネットワーク通信（たとえばＩＰ）、広帯域通信（たとえばＤＯＣＳＩＳおよびＤＳＬ）、ストレージ通信（たとえばファイバ・チャネル、ｉＳＣＳＩ）など、１つまたは複数の通信チャネルを通じた通信をサポートする。単一の接続として描写しているが、通信チャネル１２５、１５５、および１８５は任意の数でも、または通信チャネルの組み合わせでもよいことを理解されるだろう。
【００３５】
高速化ミドルボックス１５０は、静的ファイル・チャンクの重複排除が可能な任意の装置の場合がある。特に、高速化ミドルボックスは、アプリケーション・サーバから暗号化された静的ファイル・チャンクをキャッシュし、異なるクライアントが同じ静的ファイル・チャンクを要求する場合、静的ファイル・チャンク全体がネットワーク１３０を通過することを必要とせずに、静的ファイル・チャンクを配布する。ここでは２つの高速化ミドルボックスを示しているが、システム１００は、より多くの高速化ミドルボックスを含むことができることを理解されるだろう。
【００３６】
ネットワーク１３０は、任意の数のエッジ・ノードおよびネットワーク・デバイスならびに任意の数および構成のリンクを含む。さらに、ネットワーク１３０は、ＬＴＥ、ＧＳＭ、ＣＤＭＡ、ローカル・エリア・ネットワーク（ＬＡＮ）、ワイヤレス・ローカル・エリア・ネットワーク（ＷＬＡＮ）、ワイド・エリア・ネットワーク（ＷＡＮ）、メトロポリタン・エリア・ネットワーク（ＭＡＮ）など、任意の組み合わせおよび任意の数のワイヤレス、ワイヤー・ライン、またはフェムトセルのネットワークを含むことができることを理解されるだろう。
【００３７】
クライアント１８０は、クライアント通信チャネル１８５の１つまたは複数を通じてファイル／ファイル・チャンクを送信または受信できる任意のタイプの通信デバイスを含むことができる。たとえば、通信デバイスは、シン・クライアント、スマートフォン（たとえばクライアント１８０－ｃ）、パーソナル・コンピュータまたはラップトップ・コンピュータ（たとえばクライアント１８０－ａ）、サーバ（たとえば１８０－ｂ）、ネットワーク・デバイス、タブレット、テレビのセットトップ・ボックス、メディア・プレイヤなどの場合がある。通信デバイスは、処理または記憶などタスクの一部を実行するために、代表的なシステム内の他のリソースに依存する場合があるか、またはタスクを独立して実行することができる場合がある。ここでは３つのクライアントを示しているが、システム１００は、より少ないまたはより多いクライアントを含むことができる。さらに、クライアントは、操作の間の様々なときにシステムに追加または削除できるため、クライアントの数はいつでも動的な場合がある。
【００３８】
一部の実施形態では、高速化ミドルボックス１５０は、従来のＷＡＮ高速化ミドルボックスの場合がある。
【００３９】
高速化ミドルボックス１５０は、明瞭さのためにネットワーク１３０の外部に描写しているが、一部の実施形態では、高速化ミドルボックス１５０は、ネットワーク１３０内に

ある場合がある。

【００４０】

一部の実施形態では、高速化ミドルボックス１５０は、アプリケーション・サーバ１２０から受信された静的ファイル・チャンクと動的ファイル・チャンクを区別する。

【００４１】

一部の実施形態では、アプリケーション・サーバ１２０は、プロトコルを介して、高速化ミドルボックス１５０－ａ、高速化ミドルボックス１５０－ｂ、または１つまたは複数のクライアント１８０と通信する。アプリケーション・サーバは、送信されたファイル・チャンクが静的か動的かなど、アプリケーション・サーバと高速化ミドルボックスまたはクライアントとの間で適切なメッセージを通信することができ、高速化方式を適用する方法を指定するか、または圧縮方式を適用する方法を指定する。このプロトコルの一部の実施形態では、アプリケーション・サーバは、パケットの形でデータを送信し、パケット内にメッセージを含む。これらの実施形態の一部では、メッセージは、受信する高速化ミドルボックスまたはクライアントが静的または動的としてファイル・チャンクを処理するべきかどうかを指定することができる。これらの実施形態の一部では、アプリケーション・サーバおよびクライアントのペアは、従来のエンド・ホスト圧縮方式を使用することができる。本実施形態では、クライアントは、メッセージに基づくエンド・ホスト圧縮方式の実装の場合がある。たとえば、静的ファイル・チャンクは、高速化ミドルボックスによって高速化されるため、クライアントは、エンド・ホスト圧縮を使用して動的ファイル・チャンクを圧縮し、圧縮されていない静的ファイル・チャンクを送信することができる。これらの実施形態の一部では、メッセージは、暗号化されたファイル・チャンクと同じ情報単位（たとえばパケット）の一部の場合がある。これらの実施形態の一部では、メッセージ・チャンクは、暗号化されたファイル・チャンクとは異なる情報単位（たとえばパケット）の場合がある。たとえば、先頭または末尾のパケットは、１つまたは複数の後続または引き続くパケットが静的または動的なファイル・チャンクを含むことを示すメッセージを含む場合がある。

【００４２】

一部の実施形態では、高速化ミドルボックス１５０は、処理せずに動的ファイル・チャンクを渡す。

【００４３】

図２は、図１の高速化接続システム１００が、ユーザごとに暗号化されたデータを含むファイルの送信を提供するための方法２００の実施形態を示すフローチャートである。方法は、アプリケーション・サーバによるファイルのファイル・チャンクを暗号化および送信（ステップ２２０）、高速化ミドルボックスによる送信されたファイル・チャンクに高速化方式を適用（ステップ２４０）、およびクライアントによる送信されたファイル・チャンクを受信および復号化（ステップ２６０）を含む。

【００４４】

方法２００では、ステップ２２０は、アプリケーション・サーバ（たとえば図１のアプリケーション・サーバ１２０）によるターゲット・ファイルのファイル・チャンクの暗号化および送信を含む。特に、アプリケーション・サーバは、クライアント（たとえば図１のクライアント１８０の１つ）からターゲット・ファイルに対する要求を受信し、１つまたは複数の静的ファイル・チャンクおよび１つまたは複数の動的ファイル・チャンクへとターゲット・ファイルを分割し、高速化ミドルボックス（たとえば、図１の高速化ミドルボックス１５０－ａ）を介して要求側クライアントに分割されたファイル・チャンクを送信する。

【００４５】

方法２００では、ステップ２４０は、高速化ミドルボックス（たとえば、図１の高速化ミドルボックス１５０－ａおよび１５０－ｂ）による送信された暗号化されたファイル・チャンクへの高速化方式の適用を含む。高速化方式は、受信された暗号化された静的ファイル・チャンクを対応する識別子に置き換える。繰り返されるバイト・シーケンス（たと

えば静的ファイル・チャンク）を次の送信で識別子に置き換えることによって、アプリケーション遅延または帯域幅を減らすことができることを理解されるだろう。

【００４６】

方法２００では、ステップ２６０は、クライアント（たとえばクライアント１８０の１つ）による送信された暗号化されたファイル・チャンクの受信および復号化を含む。特に、受信するクライアントは、適切な鍵を用いて、適切な受信された暗号化された静的ファイル・チャンクおよび暗号化された動的ファイル・チャンクを復号化し、ターゲット・ファイルを再構築する。

【００４７】

有利なことに、ネットワークの従来のネットワーク要素は、ネットワークにおいて変更を必要とすることなく、暗号化された静的ファイル・チャンクの暗号化されたトラフィックにおける冗長性を除去することができる。さらに、動的ファイル・チャンク（たとえば個人データ）は、これらのネットワーク要素によって格納されることを必要としない。たとえば、同じファイル（たとえばウェブ・ページ）に対する２つのクライアント要求について、ネットワーク（たとえば図１つのネットワーク１３０）を通じて動的ファイル・チャンクのみを送信する必要がある一方、静的ファイル・チャンクは、クライアントに隣接する高速化ミドルボックス（たとえば図１の高速化ミドルボックス１５０－ｂ）からクライアントに送信することができる。さらに、セキュリティ（たとえば暗号化）は、静的および動的なファイル・チャンクの両方に適用することができる。

【００４８】

図３は、図２のステップ２２０に示すように、アプリケーション・サーバ（たとえば図１のアプリケーション・サーバ１２０）がターゲット・ファイルを暗号化および送信するための方法３００の実施形態を示すフローチャートである。方法は、ファイル・チャンクへとターゲット・ファイルを分割するステップ（ステップ３２０）と、適切な分割されたファイル・チャンクについて（ステップ３６０）、ファイル・チャンクが動的かどうかに基づいて（ステップ３３０）、静的な暗号化方式（ステップ３４０）または動的な暗号化方式（ステップ３５０）を適用するステップとを含む。最後に、方法は、ターゲット・クライアント（たとえば図１のクライアント１８０の１つ）にファイル・チャンクを送信する（ステップ３７０）。

【００４９】

方法３００では、ステップ３２０は、チャンクへとターゲット・ファイルを分割するステップを含む。特に、方法を実行する装置は、クライアント（たとえば図１つのクライアント１８０の１つ）からターゲット・ファイルに対する要求を受信し、１つまたは複数の静的ファイル・チャンク（つまり静的データ）および１つまたは複数の動的ファイル・チャンク（つまり動的データ）へとターゲット・ファイルを分割する。静的ファイル・チャンクは、多数のユーザに共通し一時的でないデータを含むことができる。動的ファイル・チャンクは、ユーザごとに異なるデータ、または一時的なデータを含むことができる。例として代表的なウェブ・ページを使用すると、静的ファイル・チャンクは、（ｉ）画像、（ｉｉ）メタデータ・ファイルで見つかるような共通のｈｔｍｌ；テンプレート、ヘッダー、フッター、およびメニュー、（ｉｉｉ）ｃｓｓファイルなどのスタイル・シート・ファイル、（ｉｖ）ｊａｖａｓｃｒｉｐｔまたはｊａｖａのファイルなどスクリプト・ファイル、（ｖ）その他を含むことができる。さらに、動的ファイル・チャンクは、（ｉ）ソーシャル・ネットワーキング・サイトのメッセージまたは電子商取引サイトの購入品などの個人データ、（ｉｉ）アカウント情報、発注情報など、ユーザによって以前に入力されたＨＴＭＬ形式の情報、（ｉｉｉ）検索の結果などウェブ・ページのカスタマイズされた部分、（ｉｖ）株式相場表示機など一時データ、または（ｖ）その他を含むことができる。

【００５０】

方法３００に、ステップ３３０は、分割されたファイル・チャンクの１つが動的データを含むかどうかを判定するステップを含む。ファイル・チャンクが動的データを含む場合

、方法はステップ３５０に進み、そうでなければ方法はステップ３４０に進む。
【００５１】
方法３００では、ステップ３４０は、分割された静的ファイル・チャンクの１つに静的な暗号化方式を適用するステップを含む。特に、静的な暗号化方式は、異なるクライアントに対して同一の暗号化された静的ファイル・チャンクを作成する。
【００５２】
方法３００では、ステップ３５０は、分割されたファイル・チャンクの１つに動的な暗号化方式を適用するステップを含む。特に、動的な暗号化方式は、異なるクライアントに対して同一または同一でない可能性がある暗号化された動的ファイル・チャンクを作成する。一部の実施形態では、動的な暗号化方式は対称鍵暗号化である。
【００５３】
方法３００では、ステップ３６０は、追加的なファイル・チャンクがあるかどうかを判定するステップを含む。追加的なファイル・チャンクが存在する場合、方法はステップ３３０に進み、そうでない場合は、方法はステップ３７０に進む。
【００５４】
方法３００は、必要に応じて、ステップ３７０を含む。ステップ３７０は、ターゲット・クライアントに暗号化された静的および動的なファイル・チャンクを送信するステップを含む。
【００５５】
一部の実施形態では、ステップ３２０は、動的または個々のクライアントにとって個人的なファイル・チャンク（つまり動的データ）から静的かつ複数のクライアントに「共通」するファイル・チャンク（つまり静的データ）を分割するステップを含む。
【００５６】
ステップ３２０の一部の実施形態では、ファイルの「個人的な」データは、１つまたは複数の動的ファイル・チャンクへと分割される。個人データは機密性があり、ユーザごとに異なる。有利なことに、個人データは、セキュリティ・プロパティを損なわないように暗号化することができ、しかも従来のＷＡＮ高速化ミドルボックスは、静的ファイル・チャンクに対して冗長性消去を実行することができる。
【００５７】
一部の実施形態では、ステップ３２０および３６０は、機能を共有することができる。たとえば、ステップ３２０は、完全な組のファイル・チャンクへとターゲット・ファイルを分割しない場合がある。本実施形態では、ステップ３６０は、ターゲット・ファイルから次のファイル・チャンクを分割することができる。
【００５８】
ステップ３３０の一部の実施形態では、ステップ３４０または３５０の暗号化方式の１つを使用して、分割されたファイル・チャンクを暗号化する必要がないことを判定することができ、次に、ステップ３４０または３５０のどちらかを適用せずに、方法はステップ３６０に進むことができる。
【００５９】
一部の実施形態では、ステップ３４０は、静的ファイル・チャンクを暗号化するために収束暗号化（ＣＥ）を使用するステップを含む。収束暗号化は、コンテンツ自体（たとえば静的ファイル・チャンク）から鍵を取得し、コンテンツ（たとえば静的ファイル・チャンク）を暗号化するために、その取得した鍵を使用する。たとえば、静的ファイル・チャンクｂについて、静的ファイル・チャンクｂは、鍵ｋ＝Ｈ（ｂ）を用いて暗号化することができる。有利なことに、同じ静的ファイル・チャンク（たとえばウェブ・ページのプレーン・テキスト）は、同一の暗号化された静的ファイル・チャンクを作成する、同じ鍵を使用して暗号化される。したがって、次に、同一の暗号化された静的ファイル・チャンクは、従来のＷＡＮ高速化ソリューションを使用して高速化することができる。
【００６０】
ステップ３４０の一部の実施形態では、収束するように暗号化された静的ファイル・チ

ャンクを復号化するための鍵は、個別の暗号化方式を介して送信される。これらの実施形態の一部では、鍵は、クライアントにＨＴＴＰＳを介して送信される。

【００６１】

一部の実施形態では、ステップ３４０は、アプリケーション・レイヤで暗号化方式を適用するステップを含む。有利なことに、これらの実施形態の一部では、他のネットワーク要素は、暗号化された静的ファイル・チャンクをプレーンテキスト・データとして処理し、暗号化された静的ファイル・チャンクの上に既存の方式を適用して、従来のＷＡＮ高速化ソリューションの完全な利点を可能にすることができる。

【００６２】

ステップ３５０の一部の実施形態では、対称鍵暗号はＨＴＴＰＳである。たとえば、ＨＴＴＰＳ接続は、ＨＴＴＰＳプロトコルによって生成されたユーザごとの対称鍵で暗号化された、暗号化された動的ファイル・チャンクを含む。

【００６３】

方法３００の一部の実施形態では、ステップ３４０で静的ファイル・チャンクを復号化するための鍵は、ステップ３５０の暗号化された動的ファイル・チャンクの少なくとも１つの中に含まれている。

【００６４】

方法３００の一部の実施形態では、ステップ３３０および３６０は、同時に実行することができる。たとえば、ステップ３６０で、ステップ３４０、３５０、または３７０に進むかどうかについて第３の判定を行うことができる。

【００６５】

一部の実施形態では、ステップ３７０は、各暗号化ステップ（たとえば３４０または３５０）の後に発生する場合があり、すべてのファイル・チャンクがステップ３６０を介して分析されるまで待つ必要はない。

【００６６】

一部の実施形態では、ステップ３７０は、ＴＣＰ／ＩＰまたはＨＴＴＰＳの使用により送信するステップを含む。

【００６７】

図４は、図２のステップ２４０に示すように、１対の高速化ミドルボックス（たとえば、図１の高速化ミドルボックス１５０－ａおよび１５０－ｂ）が高速化方式を提供するための方法４００の実施形態を示すフローチャートを示している。方法は、第１の装置によって実行される部分４１０－ａ（たとえば、図１の高速化ミドルボックス１５０－ａ）および第２の装置によって実行される部分４１０－ｂ（たとえば、高速化ミドルボックス１５０－ｂ）を含む。

【００６８】

第１の装置は、アプリケーション・サーバ（たとえば、図１のアプリケーション・サーバ１２０）からファイル・チャンクを受信し（ステップ４２０）、ファイル・チャンクに高速化方式を適用するべきかどうかを判定する（ステップ４４０）。高速化方式が適用されないと第１の装置が判定した場合、第１の装置は、受信されたファイル・チャンクを第２の装置に送信する（ステップ４４２）。高速化方式が適用されると第１の装置が判定した場合、第１の装置は、ファイル・チャンクに対してファイル・チャンク識別子が存在するかどうかを判定する（ステップ４５０）。ファイル・チャンクに対してファイル・チャンク識別子が存在しない場合、第１の装置は、ファイル・チャンク識別子を決定し、第２の装置にファイル・チャンクおよびその関連するファイル・チャンク識別子を送信する（ステップ４６２）。ファイル・チャンクに対するファイル・チャンク識別子が存在する場合、第１の装置は、第２の装置にファイル・チャンク識別子を送信する（ステップ４８２）。

【００６９】

第２の装置は、ファイル・チャンクを受信するか（ステップ４４４）、ファイル・チャンクおよびファイル・チャンク識別子を受信するか（ステップ４６４）、または第１の装

置からファイル・チャンク識別子を受信し（ステップ４８４）、次にクライアントにファイル・チャンクを送信する（ステップ４９０）。第２の装置がファイル・チャンクおよびファイル・チャンク識別子を受信すると（ステップ４６４）、第２の装置は、ファイル・チャンクの送信に加えて、ファイル・チャンク－ファイル・チャンク識別子の関連を格納する（ステップ４６６）。第２の装置がファイル・チャンク識別子のみを受信すると（ステップ４８４）、第２の装置は、ファイル・チャンクの送信に加えて、ファイル・チャンク－ファイル・チャンク識別子の関連に基づいて、格納されたファイル・チャンクを取得する（ステップ４８６）。

【００７０】

ステップ４６６または４８６の一部の実施形態では、ファイル・チャンク－ファイル・チャンク識別子は、表で関連づけることができる。

【００７１】

ステップ４６２および４６４の一部の実施形態では、ファイル・チャンク識別子は、ファイル・チャンクと共に送信されない。これらの実施形態では、第２の装置が、格納されたファイル・チャンク－ファイル・チャンク識別子の関連を持っていない場合、第２の装置は、ファイル・チャンクに基づいてファイル・チャンク識別子を決定し、ステップ４６６で、決定されたファイル・チャンク識別子を格納する。第２の装置は、ファイル・チャンクのコンテンツに基づいてファイル・チャンク識別子を決定できるため、ファイル・チャンク識別子がファイル・チャンク・コンテンツに基づいている場合、ファイル・チャンク識別子は、第１の装置によって送信される必要はないことを理解されるだろう。

【００７２】

ステップ４８２の一部の実施形態では、第１の装置は、また、ファイル・チャンクを送信することができる。これらの実施形態の一部では、第１の装置は、ファイル・チャンク識別子の期限が切れたと判定することができる。これらの実施形態の一部では、第１の装置は、第２の装置が、格納された関連するファイル・チャンク－ファイル・チャンク識別子を持っていないと判定することができる。たとえば、第１の装置が、ファイル・チャンク－ファイル・チャンク識別子をまだ以前に受信していない高速化ミドルボックスである場合、または第１の装置が、第２の装置が格納された関連を持っていないという指示を受信した場合である。これらの実施形態の一部では、第２の装置は、第２の装置が受信されたファイル・チャンク識別子に対する関連を持っていないという応答メッセージを第１の装置に送信し、次にメッセージに応じて、第１の装置は、ファイル・チャンクを送信し、必要に応じて、ファイル・チャンク識別子を再送することができる。

【００７３】

主に特定の順序で描写および記述しているが、方法２００、３００、および４００に示したステップは、任意の適切な順序で実行できることを理解されたい。さらに、１つのステップによって識別されるステップは、また、連続する１つまたは複数の他のステップで実行することができるか、または２つ以上のステップの共通する動作は、１度のみ実行することができる。

【００７４】

上記の様々な方法のステップは、プログラムされたコンピュータによって実行することができることを理解されるだろう。本明細書において、一部の実施形態は、また、機械またはコンピュータで読み取り可能であり、装置で実行可能またはコンピュータで実行可能なプログラム命令をエンコードする、たとえば、データ記憶メディアなど、プログラム記憶装置を包含することを意図するものであり、前述の命令は、上記方法のステップの一部またはすべてを実行する。プログラム記憶装置は、たとえば、デジタル・メモリ、磁気ディスクや磁気テープなどの磁気記憶メディア、ハード・ドライブ、または光学的に読み取り可能なデータ記憶メディアなどでもよい。また、実施形態は、上記方法の前記ステップを実行するようにプログラムされたコンピュータを包含することを意図するものである。

【００７５】

図５は、図１のアプリケーション・サーバ１２０または図１の高速化ミドルボックス１

５０の１つなど、様々な装置５００の実施形態を概略的に示している。装置５００は、プロセッサ５１０、データ記憶装置５１１、およびＩ／Ｏインターフェース５３０を含む。

【００７６】

プロセッサ５１０は、装置５００の操作を制御する。プロセッサ５１０は、データ記憶装置５１１と協働する。

【００７７】

データ記憶装置５１１は、必要に応じて、ルーティング情報などのプログラム・データを格納することができる。データ記憶装置５１１は、また、プロセッサ５１０によって実行可能なプログラム５２０を格納する。

【００７８】

プロセッサで実行可能なプログラム５２０は、Ｉ／Ｏインターフェース・プログラム５２１、ファイル・サービス・プログラム５２３、またはファイル・チャンク高速化プログラム５２５を含むことができる。プロセッサ５１０は、プロセッサで実行可能なプログラム５２０と協働する。

【００７９】

Ｉ／Ｏインターフェース５３０は、必要に応じてかつ上記のように、図１の通信チャネル１２５および１５５を通じて通信をサポートするために、プロセッサ５１０およびＩ／Ｏインターフェース・プログラム５２１と協働する。

【００８０】

ファイル・サービス・プログラム５２３は、上記のように図３の方法３００のステップを実行する。

【００８１】

ファイル・チャンク高速化プログラム５２５は、上記のように図４の方法４００の部分４１０－ａまたは４１０－ｂのステップを実行する。

【００８２】

一部の実施形態では、プロセッサ５１０は、プロセッサ／ＣＰＵコアなどのリソースを含むことができ、Ｉ／Ｏインターフェース５３０は、任意の適切なネットワーク・インターフェースを含むことができ、またはデータ記憶装置５１１は、メモリもしくは記憶デバイスを含むことができる。さらに、装置５００は、１つまたは複数のサーバや、プロセッサ、メモリ、ネットワーク・インターフェース、または記憶デバイスなどのコンポーネントから構成されるブレードなど任意の適切な物理ハードウェア構成の場合がある。これらの実施形態の一部では、装置５００は、相互にリモートであるクラウド・ネットワーク・リソースを含むことができる。

【００８３】

一部の実施形態では、装置５００は、バーチャル・マシンの場合がある。これらの実施形態の一部では、バーチャル・マシンは、異なるマシンからのコンポーネントを含む場合も、または地理的に分散している場合もある。たとえば、データ記憶装置５１１およびプロセッサ５１０は、２台の異なる物理的なマシンにある場合がある。

【００８４】

プロセッサで実行可能なプログラム５２０がプロセッサ５１０に実装される場合、特定の論理回路と同様に動作する一意のデバイスを提供するために、プログラム・コード・セグメントはプロセッサに組み合わせられる。

【００８５】

本明細書における描写および記述は、たとえば、プログラムおよびロジックはデータ記憶装置内に格納され、メモリは、プロセッサに通信できるように接続されている実施形態に関するが、そのような情報は、任意の適切な配置のデバイスに通信できるように接続されたメモリ、記憶装置、もしくはデータベースの任意の適切な配置を使用して、メモリ、記憶装置、もしくは内部もしくは外部のデータベースの任意の適切な組み合わせに情報を格納して、または任意の適切な数のアクセス可能な外部メモリ、記憶装置、もしくはデータベースを使用して、任意の他の適切な方法で（たとえば、任意の適切な数のメモリ、記

憶装置、またはデータベースを使用して）格納できることを理解されたい。したがって、本明細書で言及するデータ記憶装置という用語は、メモリ、記憶装置、およびデータベースの適切な組み合わせをすべて包含することを意図している。

【００８６】

記述および図面は、単に本発明の原理を示すものである。本明細書に明示的に記述して示していないが、本発明の原理を具体化し、その精神および範囲に含まれる様々な配置を当業者であれば考案できることを理解されるだろう。さらに、本明細書に詳述したすべての例は、原則として、読者が本発明の原理、およびその技術を推進する発明者（ら）によって提供された概念を理解するのを支援するために、教育のみを目的とすることを明確に意図するものであり、そのような具体的に詳述された例および条件に限定しないものとして解釈するべきである。さらに、本明細書において、本発明の原理、態様、および実施形態を詳述するすべての記述、およびその特定の例は、その等価物を包含することを意図するものである。

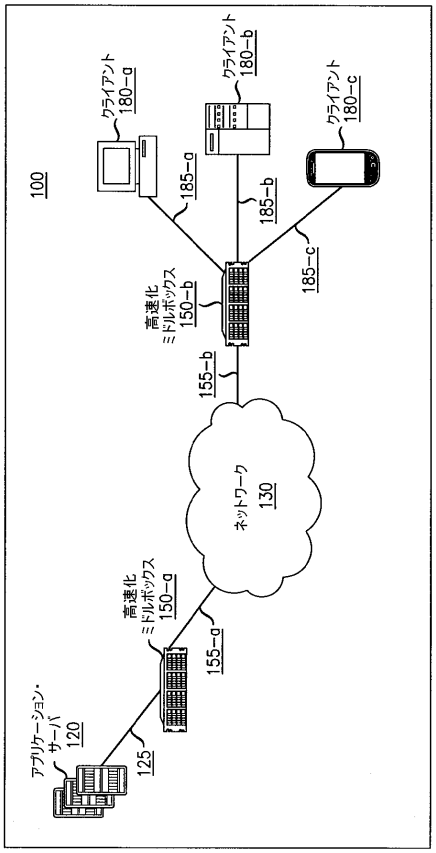
【００８７】

「プロセッサ」と書かれた任意の機能ブロックを含む、図に示す様々な要素の機能は、専用ハードウェア、および適切なソフトウェアと連携してソフトウェアを実行する機能を持つハードウェアの利用を通じて提供することができる。プロセッサによって提供される場合、機能は、単一の専用プロセッサによって、単一の共有プロセッサによって、またはその一部を共有できる、複数の個々のプロセッサによって提供することができる。さらに、「プロセッサ」または「コントローラ」という用語の明示的な使用は、ソフトウェアを実行できるハードウェアを排他的に指すものと解釈するべきではなく、デジタル・シグナル・プロセッサ（ＤＳＰ）ハードウェア、ネットワーク・プロセッサ、特定用途向けＩＣ（ＡＳＩＣ）、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、ソフトウェアを格納するための読み取り専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、および不揮発性記憶装置を限定することなく、暗黙的に含むことができる。従来型またはカスタムの他のハードウェアも含むことができる。同様に、図に示すすべてのスイッチは概念のみを示すものである。それらの機能は、プログラム・ロジックの動作を通じて、専用ロジックを通じて、プログラム制御および専用ロジックの対話を通じて、または手動でも、実行することができ、内容からより明確に理解されるように、特定の技術を実装者が選択可能である。

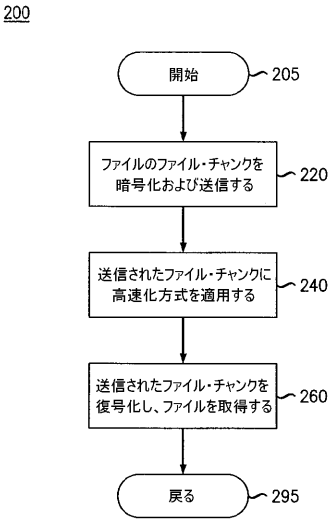
【００８８】

本明細書に示すブロック図は、本発明の原理を具体化する実例となる回路についての概念的な視点を表していることは自明であろう。同様に、そのようなコンピュータまたはプロセッサが明示的に示されているかどうかに関わりなく、任意のフローチャート、流れ図、状態遷移図、擬似コードなどは、コンピュータ可読媒体において本質的に表され、したがって、コンピュータまたはプロセッサによって実行できる様々なプロセスを表していることを理解されたい。

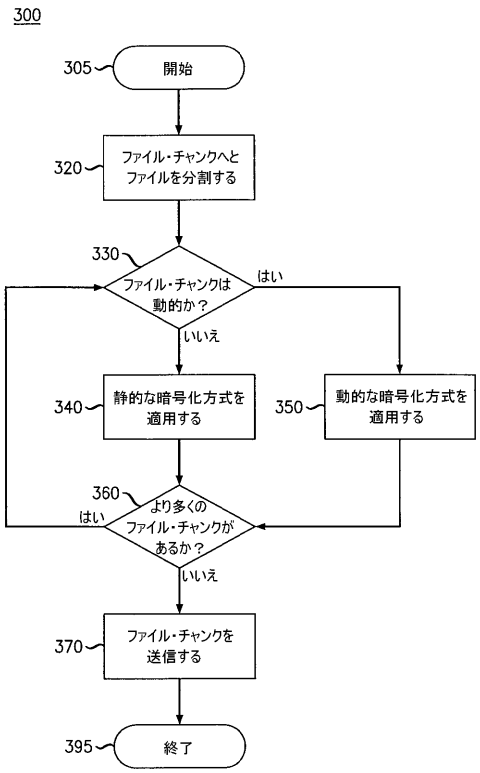
【図１】


100
クライアント 180−a
クライアント 180−b
クライアント 180−c
185−a
185−b
185−c
高速化ミドルボックス 150−b
155−b
ネットワーク 130
高速化ミドルボックス 150−a
155−a
アプリケーション・サーバ 120
125

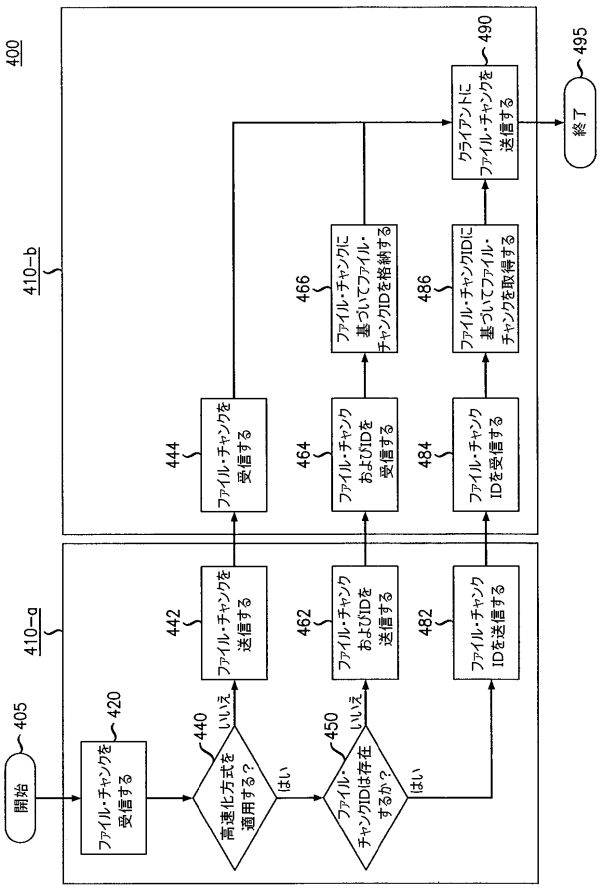
【図２】


200
開始 205
ファイルのファイル・チャンクを暗号化および送信する 220
送信されたファイル・チャンクに高速化方式を適用する 240
送信されたファイル・チャンクを復号化し、ファイルを取得する 260
戻る 295

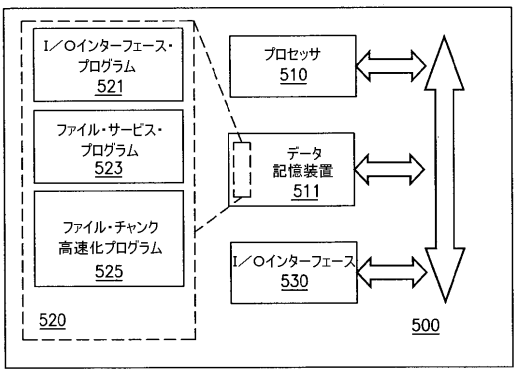
【図３】


300
305 開始
320 ファイル・チャンクへとファイルを分割する
330 ファイル・チャンクは動的か？
はい
いいえ
340 静的な暗号化方式を適用する
350 動的な暗号化方式を適用する
360 より多くのファイル・チャンクがあるか？
はい
いいえ
370 ファイル・チャンクを送信する
395 終了

【図４】


400
410−a
410−b
405 開始
420 ファイル・チャンクを受信する
440 高速化方式を適用する？
いいえ
はい
450 ファイル・チャンクIDは存在するか？
いいえ
はい
442 ファイル・チャンクを送信する
462 ファイル・チャンクおよびIDを送信する
482 ファイル・チャンクIDを送信する
444 ファイル・チャンクを受信する
464 ファイル・チャンクおよびIDを受信する
484 ファイル・チャンクIDを受信する
466 ファイル・チャンクに基づいてファイル・チャンクIDを格納する
486 ファイル・チャンクIDに基づいてファイル・チャンクを取得する
490 クライアントにファイル・チャンクを送信する
495 終了

【図５】


500
I／Oインターフェース・
プログラム
521
ファイル・サービス・
プログラム
523
ファイル・チャンク
高速化プログラム
525
520
プロセッサ
510
データ
記憶装置
511
I／Oインターフェース
530
500

フロントページの続き

(72)発明者 プッタスァミ ナガ, クリシュナ, ピー.
アメリカ合衆国 ０８８３７ ニュージャーシィ, エジソン, コスター ブールバール １２, アパートメント ３ビー
(72)発明者 グオ, キャサリン
アメリカ合衆国 ０７９７４－０６３６ ニュージャーシィ, マレイ ヒル, マウンテン アヴェニュー ６００－７００

審査官 金沢 史明

(56)参考文献 特表２００５－５１３６４０（ＪＰ, Ａ）
特開２００３－２６３３８５（ＪＰ, Ａ）
米国特許出願公開第２０１０／０３３２５８７（ＵＳ, Ａ１）
特開２０１２－８３９１０（ＪＰ, Ａ）
特開２００３－１３１９２９（ＪＰ, Ａ）
米国特許出願公開第２００２／０１８４４８８（ＵＳ, Ａ１）
米国特許出願公開第２００３／００５５８８１（ＵＳ, Ａ１）
特開２００６－１７９００７（ＪＰ, Ａ）
米国特許出願公開第２００９／０２５４７０７（ＵＳ, Ａ１）
Y. Song et al., Multiple-channel security architecture and its implementation over SSL, EURASIP Journal on Wireless Communications and Networking, Hindawi Publishing Corp., ２００６年 4月, Volume 2006, Issue 2, Article ID 85495, pp. 1-14

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／００－ ９／３８
Ｇ０６Ｆ １２／００
Ｇ０６Ｆ １３／００