(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2015-103933
(P2015-103933A)
(43)公開日　平成27年6月4日(2015.6.4)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/18	(2006.01)	H04L	9/00	651	5J104
H04L	12/22	(2006.01)	H04L	12/22		5K030
H04L	12/717	(2013.01)	H04L	12/717		

審査請求 未請求　請求項の数 12　ＯＬ　（全 28 頁）

(21)出願番号　特願2013-242470 (P2013-242470)
(22)出願日　平成25年11月25日 (2013.11.25)

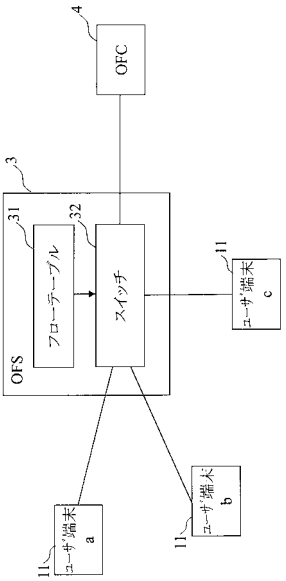
（出願人による申告）平成２３年度、独立行政法人情報通信研究機構、「高速通信・放送研究開発委託研究／高機能光電子融合型パケットルータ基盤技術の研究開発」、産業技術力強化法第１９条の適用を受ける特許出願

(71)出願人　800000068
学校法人東京電機大学
東京都足立区千住旭町５番
(74)代理人　100119677
弁理士　岡田　賢治
(74)代理人　100115794
弁理士　今下　勝博
(72)発明者　宮保　憲治
東京都足立区千住旭町５番　学校法人東京電機大学内
(72)発明者　上野　洋一郎
東京都足立区千住旭町５番　学校法人東京電機大学内

最終頁に続く

(54)【発明の名称】ネットワーク制御システム及び方法

(57)【要約】
【課題】本発明は、ホスト間またはホストーサーバ間での暗号化及び復号化を行う方式から脱却し、ＳＤＮの通信ノード内のスイッチで暗号化等の処理を自律的に、かつ第３者には秘密の方法で実施することにより、第３者に対する通信の機密性を確保するとともに、ユーザ端末の負荷を減らすことを目的とする。
【解決手段】本発明に係るネットワーク制御システム及びネットワーク制御方法は、ＳＤＮの通信ノード内のスイッチで暗号化等の通信の機密性を確保するための処理を行い、スイッチと専用通信ネットワークで接続されたＳＤＮのコントローラにおいてスイッチの行った処理に関するパラメータやメタデータを管理する。
【選択図】図５



【特許請求の範囲】
【請求項１】
コントローラからのソフトウェア制御を用いてスイッチの出力経路を制御するネットワーク制御システムにおいて、
前記スイッチは、ユーザ端末からの通信データを受信すると、当該通信データを複数の断片データに分割して断片データの配列順を変更し、配列順を変更後の各断片データを、出力経路を制御するためのフローテーブルに従った出力経路に向けて出力するとともに、専用通信ネットワークを用いて変更後の前記断片データの配列順を前記コントローラに出力し、
前記コントローラは、変更後の前記断片データの配列順を格納する、
ネットワーク制御システム。
【請求項２】
前記スイッチは、ユーザ端末から通信のデータを符号化して当該通信データを複数の断片データに分割するか、或いはユーザ端末からの通信データを複数の断片データに分割して各断片データを符号化するとともに、前記専用通信ネットワークを用いて前記スイッチで行った符号化を復号化するために必要なメタデータを前記コントローラに出力し、
前記コントローラは、前記スイッチで符号化された通信データを復号化するために必要なメタデータをさらに格納する
ことを特徴とする請求項１に記載のネットワーク制御システム。
【請求項３】
前記スイッチは、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信すると、前記コントローラに格納されている前記メタデータに従って前記通信データ又は前記断片データを復号化する
請求項２に記載のネットワーク制御システム。
【請求項４】
前記スイッチは、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信すると、前記コントローラに格納されている前記メタデータを当該ユーザ端末へ送信し、
当該ユーザ端末は、前記スイッチから取得するメタデータを用いて前記通信データ又は前記断片データを復号化する
請求項２に記載のネットワーク制御システム。
【請求項５】
前記スイッチは、ユーザ端末から通信データの取得要求を受信すると、当該通信データを構成する複数の断片データの配列順を前記コントローラに格納されている配列順に従って変更し、配列順を変更後の断片データの集合を、当該ユーザ端末へ送信する
ことを特徴とする請求項１から４のいずれかに記載のネットワーク制御システム。
【請求項６】
前記スイッチは、
ネットワークに対して要求するセキュリティサービス種別を、ユーザ端末からの前記通信データに含まれるフラグ種別情報から識別し、
前記セキュリティサービス種別がバックアップ用のサービスである場合、前記フローテーブルに従った１以上のストレージ端末に向けて、前記断片データを出力するとともに、前記専用通信ネットワークを用いて前記断片データの送信先を前記コントローラに出力し、
前記コントローラは、前記断片データの送信先をさらに格納する
請求項１から５のいずれかに記載のネットワーク制御システム。
【請求項７】
コントローラからのソフトウェア制御を用いてスイッチの出力経路を制御するネットワーク制御方法において、
ユーザ端末からの通信データを受信した前記スイッチが、出力経路を制御するためのフローテーブルを参照し、当該通信データを複数の断片データに分割して断片データの配列

順を変更し、配列順を変更後の各断片データを前記フローテーブルに従った出力経路に向けて出力するとともに、専用通信ネットワークを用いて変更後の前記断片データの配列順を前記コントローラに格納するデータ送信手順を有するネットワーク制御方法。
【請求項８】
前記データ送信手順において、ユーザ端末からの通信データを受信した前記スイッチが、ユーザ端末からの通信データを符号化して当該通信データを複数の断片データに分割するか、或いはユーザ端末からの通信データを複数の断片データに分割して各断片データを符号化するとともに、前記専用通信ネットワークを用いて当該スイッチで符号化された通信データを復号化するために必要なメタデータを前記コントローラに格納する
ことを特徴とする請求項７に記載のネットワーク制御方法。
【請求項９】
ユーザ認証の完了したユーザ端末から通信データの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信するデータ受信手順を、前記データ送信手順の後にさらに有し、
前記データ受信手順において、当該スイッチが、前記コントローラに格納されている前記メタデータに従って前記通信データ又は前記断片データを復号化する
ことを特徴とする請求項８に記載のネットワーク制御方法。
【請求項１０】
ユーザ認証の完了したユーザ端末から通信データの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信するデータ受信手順を、前記データ送信手順の後にさらに有し、
前記データ受信手順において、当該スイッチが、前記コントローラに格納されている前記メタデータを当該ユーザ端末へ送信し、前記スイッチからメタデータを取得した当該ユーザ端末が当該メタデータを用いて前記通信データ又は前記断片データを復号化する
ことを特徴とする請求項８に記載のネットワーク制御方法。
【請求項１１】
ユーザ認証の完了したユーザ端末から通信データの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信するデータ受信手順を、前記データ送信手順の後にさらに有し、
前記データ受信手順において、当該スイッチが、当該通信データを構成する複数の断片データの配列順を前記コントローラに格納されている配列順に従って変更し、配列順を変更後の断片データの集合を、当該ユーザ端末へ送信する
ことを特徴とする請求項７から１０のいずれかに記載のネットワーク制御方法。
【請求項１２】
前記データ送信手順において、
ユーザ端末からの通信データを受信した前記スイッチが、ネットワークに対して要求するセキュリティサービス種別を当該通信データに含まれるフラグ種別情報から識別し、
前記セキュリティサービス種別がバックアップ用のサービスである場合、前記フローテーブルに従った１以上のストレージ端末に向けて、前記断片データを出力するとともに、専用通信ネットワークを用いて前記断片データの送信先を前記コントローラに格納する
ことを特徴とする請求項７から１１のいずれかに記載のネットワーク制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＳＤＮスイッチを用いたネットワーク制御システム及び方法に関する。
【背景技術】
【０００２】
ソフトウェア制御が可能なネットワーク（ＳＤＮ：Ｓｏｆｔｗａｒｅ　Ｄｅｆｉｎｅｄ　Ｎｅｔｗｏｒｋ）の一つの技術要素として、ネットワークノードの機能をネットワークルーチング機構（ノードのデータ転送機能）とコントローラ機構（ノードでの制御ソフト

ウェア・ルーチング制御機能）とに、分離できるようにインタフェースを公開し、ネットワーク制御をプログラマブルにすることにより、柔軟な経路制御や構成変更、ならびに新しい通信サービス等を実現可能とするネットワーク制御機構が注目されている。ＳＤＮではコントローラがネットワーク内の全情報を集め、一元的に定義し、ソフトウェアを活用した集中制御処理に基づいて、ネットワーク全体を制御できる特徴を持つ。コントローラは、スイッチ制御用のソフトウェアを配備することにより、スイッチの動作を制御できる。

【０００３】

ＳＤＮの実現方法の１つとして、オープンフロー（ＯｐｅｎＦｌｏｗ：非特許文献１、２）と呼ばれるネットワークプラットフォームの標準化が進められ、オープンソースによる実装と同時に企業によるシステム／製品群が市場に普及しつつある。ＳＤＮを実現するスイッチやコントローラに関しては、オープンソースとして公開したＴｒｅｍａやスタンフォード大学で開発されたＢｅａｃｏｎ、Ｎｉｃｉｒｉａ Ｎｅｔｗｏｒｋ社が開発したＮＯＸ等がある。ＳＤＮを実現する上での課題の一つは、ネットワークで提供されるサービスに対して、セキュリティを高めるための有効な技術を提供することであり、このメカニズムを開示することが本発明の目的である。しかしながら、高いセキュリティを確保した高信頼なデータ配信サービスをＳＤＮの機構を適切に用いて、ネットワーク内で新たなセキュリティ基準のもとに、新しい制御機構技術として組み込んだ例は開示されていない。本発明で開示する技術は、いずれのスイッチやコントローラに対しても、同様に適用することが可能であり、高信頼のネットワークサービスを実現する上での技術基盤を提供できる。

【０００４】

特許文献１では、データファイルを分割し、当該分割された断片データを複数のクライアント端末に分散転送するバックアップ技術を用い、データファイルを保有する管理ユーザのサービス要求に見合ったセキュリティレベルでのバックアップを可能にするための技術が開示されている。

特許文献２では、各種のＰＣ端末、モバイル端末等の遊休リソースを積極的に活用し、ファイルの暗号化・分割・複製・分散化技術を組み合わせる事により、信頼性の高いディザスタリカバリを実現可能とする基本技術およびファイル一体化と呼ばれるファイルデータの撹拌技術が開示されている。

【０００５】

非特許文献１は、オープンフローコントローラが備えるべきデータを分散データベース上に構築し、オープンフローコントローラを介して実装されるネットワークアプリケーションに対して適切なＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）を提供することで、オープンフローコントローラの分散化を実現している。

非特許文献２は、データを分散データベース上で管理すると共に、複数のオープンフローコントローラ間で通信を行うことで同期をとる方法が示されている。

【０００６】

ソフトウェア制御を用いてスイッチの出力経路を制御するＳＤＮ内のスイッチと、スイッチ制御用のコントローラにより構成されるネットワーク制御システムを活用して、ファイルバックアップサービスを行う際の暗号化、分散転送、復号化をネットワーク制御装置のみにより、効率的に実施するメカニズムを開示している。具体的には、ユーザ端末（ホスト端末）が送出するパケットデータの中に、ネットワークに対して要求するセキュリティサービス種別をフラグ情報として含め、前記のスイッチに、フラグ情報を識別する機構を持たせることにより、ＳＤＮアーキテクチャを活用して、バックアップ用のサービスの中の特定のサービスレベル種別を識別し、ユーザの創出するユーザパケットを、スイッチ内で、当該のサービスレベルの程度に合わせて、適切な、暗号処理化や複製を行う。このことにより、ユーザ端末やゲートウェイでの暗号化等に関わる符号処理を大幅に削減し、ユーザ端末の通信処理用のスループットを大幅に向上することができる。このメカニズム

は、ユーザ端末側での暗号処理メカニズムを全く活用せずに、ネットワーク制御装置での当該処理メカニズムを用いることにより、第３者の盗聴が不可能な、秘密データ転送サービにも活用できる。

【０００７】

現在、ホストとなるユーザ端末やサーバの処理能力は向上しつつあるものの、セキュリティの高い通信を実現するためには、例えばユーザ端末で、共通鍵暗号の１つであるＡＥＳ暗号による処理を行う方法がある。この場合、暗号鍵の長さや送信するデータ容量が増加するにしたがって、計算量は一般的に、指数関数的に増加する。近年、通信で扱うデータ容量は増加しつつあり、セキュリティ強度を上げるためには、暗号鍵の長さを長く設定し、暗号処理に必要な計算量が増大する傾向がある。この結果、ユーザ端末での暗号処理に関わるオーバヘッドが、通信スループット等の低下に対する影響が無視できなくなる状況が生じつつある。

【０００８】

通常、ホスト－サーバ間、あるいはホスト－ホスト間における通信で、セキュリティを高めるためにＩＰＳｅｃやＳＳＬ／ＴＳＬ等のセキュリティプロトコルが導入されている。しかし、いずれのセキュリティプロトコルも、ユーザ端末における通信スループットの低下を来す。例えば、ＩＰｓｅｃはＩＰパケットのレベルで暗号化を行うことにより、２台のユーザ端末間の通信を、盗聴や改ざんから保護するためのセキュリティ技術として活用されている。

【０００９】

図１に示すようなゲートウェイをユーザ端末に隣接して設ける方法か、または、図２に示すようなＰＣ内蔵ソフトウェアをユーザ端末に組み込む用いる方法が利用されている。例えば、Ｗｉｎｄｏｗｓ（登録商標）２０００以上ではＩＰＳｅｃ機能をＩＰレイヤに標準で組み込んでいる。特に、後者の形態は、暗号化処理に起因するユーザ端末の処理能力を消費するため、高性能の通信スループットが要求される場合には、当該ゲートウェイ装置の導入コストは増加するものの、前者の使用形態が用いられる。ＩＰｓｅｃはＩＰ層で暗号化／復号化を行うため、他の暗号処理用のセキュリティプロトコルと比べて、既存のＬＡＮやインターネット対応のアプリケーションを変更すること無しに、暗号化が行える点が優れているが、通信確立までの処理オーバヘッドが大きく、ホスト－サーバ間、またはホスト－ホスト間の通信スループットが劣化するという問題点があった。

【００１０】

ＩＰｓｅｃではＡＥＳ等の共通鍵暗号を使用し、ネットワーク機器で暗号化処理を実施する手法が利用されているが、いくつかの問題点が存在する。一つは、通信開始時における設定手順が複雑な点である。ＩＰｓｅｃの通信開始時におけるシーケンスを図２、図３に示す。ＩＰｓｅｃでは、共通鍵暗号を使用してパケットデータを暗号化するため、共通鍵を事前に共有する必要がある。共通鍵情報、通信ノード間の認証を行うために、使用するパラメータを提案、鍵情報の交換をする。

【００１１】

図３はＩＰｓｅｃにおけるＩＫＥ（Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ）のフェーズ１の通信シーケンスである。フェーズ１では、継続して実施する次の通信シーケンス（フェーズ２）で行うＩＰｓｅｃに必要な共通鍵を安全に交換するためにＳＡ（Ｓｅｓｓｉｏｎ　Ａｓｓｏｃｉａｔｉｏｎ）を確立する。図４はＩＫＥのフェーズ２の通信シーケンスである。フェーズ２では実際にＩＰｓｅｃで使用するパラメータや鍵情報を交換する。安全な通信路を確保した後に、鍵を共有する方であるため、フェーズが２段階に別れ、通信開始時までのコストが大きくなり、通信スループットを低下させる原因にもなっている。一方、共通鍵を第３者に予測される危険性が少なくするため、ホスト側では鍵情報を定期的に交換する必要があるが、上記の手法を用いる必要がある。

【００１２】

これに対して、ＳＤＮ内のスイッチ（ＯＦＳ）、コントローラ（ＯＦＣ）は、予め決められた端末との接続を対象とし、かつ端末接続時には、認証を行うと共に、規定された仕

様を満足していないパケットは異常と見なし、スイッチ（ＯＦＳ）で廃棄する処理を組み込むことが容易である。このため、第３者による盗聴は困難であると共に、不正侵入等による（スイッチ動作を規定する）ファイルの改竄を起こす危険性は少ない。

【先行技術文献】

【特許文献】

【００１３】

【特許文献１】特許第４３８５１１１号公報

【特許文献２】特許第４２９６３０４号公報

【非特許文献】

【００１４】

【非特許文献１】Ｋ．Ｋｏｐｏｎｅｎ ｅｔ ａｌ．“Ｏｎｉｘ：Ａ Ｄｉｓｔｒｉｂｕｔｅｄ ｃｏｎｔｒｏｌ Ｐｌａｔｆｏｒｍ ｆｏｒ Ｌａｒｇｅ－ｓｃａｌｅ Ｐｒｏｄｕｃｔｉｏｎ Ｎｅｔｗｏｒｋｓ，”Ｉｎ ｔｈｅ Ｐｒｏｃ．ｏｆ ｔｈｅ ９ｔｈ ＵＳＥＮＩＸ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ Ｄｅｓｉｇｎ ａｎｄ Ｉｍｐｌｅｍｅｎｔａｔｉｏｎ（ＯＳＤＩ １０），Ｖａｎｃｏｕｖｅｒ，Ｃａｎａｄａ，Ｏｃｔｏｂｅｒ ２０１０

【非特許文献２】Ａ．Ｔｏｏｔｏｃｉａｎ ａｎｄ Ｙ．Ｇａｎｊａｌｉ，“ＨｙｐｅｒＦｌｏｗ：Ａ Ｄｉｓｔｒｉｂｕｔｅｄ Ｃｏｎｔｒｏｌ Ｐｌａｎｅ ｆｏｒ ＯｐｅｎＦｌｏｗ，”Ｉｎ ｔｈｅ Ｐｒｏｃ．Ｏｆ ＮＳＤＩ Ｉｎｔｅｒｎｅｔ Ｎｅｔｗｏｒｋ Ｍａｎａｇｅｍｅｎｔ Ｗｏｒｋｓｈｏｐ／Ｗｏｒｋｓｈｏｐ ｏｎ Ｒｅｓｅａｒｃｈ ｏｎ Ｅｎｔｅｒｐｒｉｓｅ Ｎｅｔｗｏｒｋｉｎｇ（ＩＮＭ／ＷＲＥＮ），Ｓａｎ Ｊｏｓｅ，ＣＡ，ＵＳＡ，Ａｐｒｉｌ ２０１０

【発明の概要】

【発明が解決しようとする課題】

【００１５】

本発明は、ホスト間またはホストーサーバ間での暗号化及び復号化を行う方式から脱却し、ＳＤＮの通信ノード内のスイッチで暗号化等の処理を自律的に、かつ第３者には秘密の方法で実施することにより、第３者に対する通信の機密性を確保するとともに、ユーザ端末の負荷を減らすことを目的とする。

【課題を解決するための手段】

【００１６】

本発明に係るネットワーク制御システム及びネットワーク制御方法は、ＳＤＮの通信ノード内のスイッチで暗号化等の通信の機密性を確保するための処理を行い、スイッチと専用通信ネットワークで接続されたＳＤＮのコントローラにおいてスイッチの行った処理に関するパラメータやメタデータを管理する。

【００１７】

具体的には、本発明に係るネットワーク制御システムは、

コントローラからのソフトウェア制御を用いてスイッチの出力経路を制御するネットワーク制御システムにおいて、

前記スイッチは、ユーザ端末からの通信データを受信すると、当該通信データを複数の断片データに分割して断片データの配列順を変更し、配列順を変更後の各断片データを、出力経路を制御するためのフローテーブルに従った出力経路に向けて出力するとともに、専用通信ネットワークを用いて変更後の前記断片データの配列順を前記コントローラに出力し、

前記コントローラは、変更後の前記断片データの配列順を格納する。

【００１８】

本発明に係るネットワーク制御システムでは、前記スイッチは、ユーザ端末から通信のデータを符号化して当該通信データを複数の断片データに分割するか、或いはユーザ端末からの通信データを複数の断片データに分割して各断片データを符号化するとともに、前記専用通信ネットワークを用いて前記スイッチで行った符号化を復号化するために必要な

メタデータを前記コントローラに出力し、前記コントローラは、前記スイッチで符号化された通信データを復号化するために必要なメタデータをさらに格納してもよい。

【００１９】

本発明に係るネットワーク制御システムでは、前記スイッチは、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信すると、前記コントローラに格納されている前記メタデータに従って前記通信データ又は前記断片データを復号化してもよい。

【００２０】

本発明に係るネットワーク制御システムでは、前記スイッチは、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信すると、前記コントローラに格納されている前記メタデータを当該ユーザ端末へ送信し、当該ユーザ端末は、前記スイッチから取得するメタデータを用いて前記通信データ又は前記断片データを復号化してもよい。

【００２１】

本発明に係るネットワーク制御システムでは、前記スイッチは、ユーザ端末から通信データの取得要求を受信すると、当該通信データを構成する複数の断片データの配列順を前記コントローラに格納されている配列順に従って変更し、配列順を変更後の断片データの集合を、当該ユーザ端末へ送信してもよい。

【００２２】

本発明に係るネットワーク制御システムでは、前記スイッチは、ネットワークに対して要求するセキュリティサービス種別を、ユーザ端末からの前記通信データに含まれるフラグ種別情報から識別し、前記セキュリティサービス種別がバックアップ用のサービスである場合、前記フローテーブルに従った１以上のストレージ端末に向けて、前記断片データを出力するとともに、前記専用通信ネットワークを用いて前記断片データの送信先を前記コントローラに出力し、前記コントローラは、前記断片データの送信先をさらに格納してもよい。

【００２３】

具体的には、本発明に係るネットワーク制御方法は、コントローラからのソフトウェア制御を用いてスイッチの出力経路を制御するネットワーク制御方法において、ユーザ端末からの通信データを受信した前記スイッチが、出力経路を制御するためのフローテーブルを参照し、当該通信データを複数の断片データに分割して断片データの配列順を変更し、配列順を変更後の各断片データを前記フローテーブルに従った出力経路に向けて出力するとともに、専用通信ネットワークを用いて変更後の前記断片データの配列順を前記コントローラに格納するデータ送信手順を有する。

【００２４】

本発明に係るネットワーク制御方法では、前記データ送信手順において、ユーザ端末からの通信データを受信した前記スイッチが、ユーザ端末からの通信データを符号化して当該通信データを複数の断片データに分割するか、或いはユーザ端末からの通信データを複数の断片データに分割して各断片データを符号化するとともに、前記専用通信ネットワークを用いて当該スイッチで符号化された通信データを復号化するために必要なメタデータを前記コントローラに格納してもよい。

【００２５】

本発明に係るネットワーク制御方法では、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信するデータ受信手順を、前記データ送信手順の後にさらに有し、前記データ受信手順において、当該スイッチが、前記コントローラに格納されている前記メタデータに従って前記通信データ又は前記断片データを復号化してもよい。

【００２６】

本発明に係るネットワーク制御方法では、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信するデータ受信手順を、前記データ送信手順の後にさらに有し、前記データ受信手順において、当該スイッチが、前記コントローラに格納されている前記メタデータを当該ユーザ

端末へ送信し、前記スイッチからメタデータを取得した当該ユーザ端末が当該メタデータを用いて前記通信データ又は前記断片データを復号化してもよい。

【００２７】

本発明に係るネットワーク制御方法では、ユーザ認証の完了したユーザ端末から通信データの取得要求を受信した前記スイッチが前記断片データの集合を当該ユーザ端末へ送信するデータ受信手順を、前記データ送信手順の後にさらに有し、前記データ受信手順において、当該スイッチが、当該通信データを構成する複数の断片データの配列順を前記コントローラに格納されている配列順に従って変更し、配列順を変更後の断片データの集合を、当該ユーザ端末へ送信してもよい。

【００２８】

本発明に係るネットワーク制御方法では、前記データ送信手順において、ユーザ端末からの通信データを受信した前記スイッチが、ネットワークに対して要求するセキュリティサービス種別を当該通信データに含まれるフラグ種別情報から識別し、前記セキュリティサービス種別がバックアップ用のサービスである場合、前記フローテーブルに従った１以上のストレージ端末に向けて、前記断片データを出力するとともに、専用通信ネットワークを用いて前記断片データの送信先を前記コントローラに格納してもよい。

【００２９】

なお、上記各発明は、可能な限り組み合わせることができる。

【発明の効果】

【００３０】

本発明によれば、ホスト間またはホストーサーバ間での暗号化及び復号化を行う方式から脱却し、ＳＤＮの通信ノード内のスイッチで暗号化等の処理を自律的に、かつ第３者には秘密の方法で実施することにより、第３者に対する通信の機密性を確保するとともに、ユーザ端末の負荷を減らすことができる。

【図面の簡単な説明】

【００３１】

【図１】ＩＰｓｅｃの利用形態の第１例を示す。
【図２】ＩＰｓｅｃの利用形態の第２例を示す。
【図３】ＩＰｓｅｃにおけるＩＫＥフェーズ１の通信シーケンスの一例を示す。
【図４】ＩＰｓｅｃにおけるＩＫＥフェーズ２の通信シーケンスの一例を示す。
【図５】実施形態１に係るネットワーク制御システムの一例を示す。
【図６】オープンフロースイッチを用いたＳＤＮの基本構成例を示す。
【図７】アクションに指定可能な制御コマンドの一例を示す。
【図８】オープンフローで定義可能なヘッダ情報の一例を示す。
【図９】実施形態１に係る受信手順における第１のシーケンスを示す。
【図１０】実施形態１に係る受信手順における第２のシーケンスを示す。
【図１１】実施形態１に係るＯＦＣとＯＦＳの制御シーケンスの一例を示す。
【図１２】チャレンジレスポンス方式による処理フローの一例を示す。
【図１３】認証が成功した場合の通信シーケンスの一例を示す。
【図１４】実施形態３に係る通信システムの第１の形態例を示す。
【図１５】実施形態３に係る通信システムの第２の形態例を示す。
【図１６】実施形態４に係る通信システムの第１の形態例を示す。
【図１７】フラグ情報の記載方法の一例を示す。
【図１８】実施形態４におけるＯＦＳ３の処理フローの一例を示す。
【図１９】ＯＦＳがＯＦＣにメタデータを問い合わせるシーケンスの一例を示す。
【図２０】ＯＦＳにおけるバッファ処理の一例を示す。
【図２１】ＯＦＳにおける符号化処理フローの一例を示す。
【図２２】ＯＦＳにおけるシャッフリング処理フローの一例を示す。
【図２３】ＯＦＳにおける復号処理の一例を示す。
【図２４】実施形態５に係る通信システムの形態例を示す。

【図２５】実施形態６に係る通信システムの形態例を示す。
【発明を実施するための形態】
【００３２】
以下、本発明の実施形態について、図面を参照しながら詳細に説明する。なお、本発明は、以下に示す実施形態に限定されるものではない。これらの実施の例は例示に過ぎず、本発明は当業者の知識に基づいて種々の変更、改良を施した形態で実施することができる。なお、本明細書及び図面において符号が同じ構成要素は、相互に同一のものを示すものとする。
【００３３】
本願発明のセキュリティネットワーク制御システムは、ソフトウェア制御を用い、スイッチの出力経路の制御に必要な情報を提供するＳＤＮコントローラ、および当該のＳＤＮの指示に基づいて動作するスイッチが共同して、新たにスイッチ内でファイルバックアップ処理をセキュアーに実現する上で必要となるメカニズムを、提供できる手段を開示する。
【００３４】
具体的には、制御用パケットに含まれるフラグ種別情報に基づいて、ＳＤＮスイッチが、ユーザから送出される要求パケットデータのセキュリティ上のサービスレベルの種別を判定し、当該レベルに適合した符号化処理（一体化処理等の暗号化、分割、シャッフリング処理および複製等）を行い、また復元時には、上記と逆の動作手順を用いることにより、当該のファイルバックアップサービスが実現できる。
【００３５】
本方式で開示する技術を活用することにより、従来ＩＰｓｅｃ等を用いてセキュリティを確保できる場合の通信サービスと同等以上のセキュリティと安全性を、当該スイッチに上記の符号化および復号化処理を行う機能を内蔵させることにより実現し、ユーザ端末からの通信スループットも向上できる。また、符号化処理に用いるパラメータと、復号処理に必要なデータ（以下、メタデータと呼称する）を、前述のＩＫＥと同様にネットワーク機器間で共有できる。本方式では、ＳＤＮの一例として活用されるオープンフロー用のネットワークプラットフォームを用い、コントローラ（ＯＦＣ）がメタデータを管理し、スイッチ（ＯＦＳ）とＯＦＣがメタデータを共有することにより、セキュアーな通信を実現できる。
【００３６】
ＯＦＣはＯＦＳあるいは他のＯＦＣのみと接続されているため、ＯＦＳおよびＯＦＣのみにより、メタデータを共有する専用通信ネットワークが必要であり、この条件により共通鍵を共有するための安全なネットワークを確立するＩＫＥのフェーズ１の手順を省略することが可能となる。ここで、専用通信ネットワークは、仮想的専用通信ネットワークでもよいし、物理的専用通信ネットワークでもよい。一般に、メタデータのデータサイズは、ファイル送受信の対象となるパケットのデータサイズと比べて、２ケタ以上に小さいため、上記の専用通信ネットワークの帯域は十分に小さい帯域の通信回線を用いて経済的に構築できる。また、従来から使用されているＩＰｓｅｃ等の通信形態では、データ通信と共通鍵の共有を同じネットワーク回線を用いるため、頻繁に鍵を交換することにより、ユーザデータの通信のスループットが低下するが、本方式ではメタデータ等の制御データを配信するための通信路とユーザのファイルデータ配信のためのデータ通信路とを分離しているため、メタデータと符号化処理されたパケットを用いた通信データを並列に送受信できる。また、頻繁にメタデータの交換が生じる場合でも、ダイナミックにＯＦＣの負荷を調整できる方式が適用可能であるため、データ通信のスループットに影響を与えることはない。
【００３７】
本発明は、クラウド等のコンピュータリソースとの通信やデータのバックアップを実行する際のネットワーク制御装置又はオープンフロー制御機構（パケット処理制御機構）を活用することにより、ネットワーク内のスイッチをインテリジェント化することにより、

安全な通信を実現する。また本発明は任意のＳＤＮコントーラに適用できるが、以下の実施形態ではＳＤＮコントローラの一例として、ＯＦＳおよびＯＦＣについて説明する。

【００３８】

（実施形態１）

図５に、本実施形態に係るネットワーク制御システムの一例を示す。本実施形態に係るネットワーク制御システムは、コントローラからのソフトウェア制御を用いてスイッチの出力経路を制御するＳＤＮを用いる。本実施形態では、ＳＤＮの基本構成の一例として、一般的なオープンフロースイッチの構成を示す。

【００３９】

オープンフロースイッチでは、従来のルータ等のネットワーク機器が持つ機能を、オープンフローコントローラ（以下、ＯＦＣと記す）４とフローテーブルの内容に基づいてパケットを転送するオープンフロースイッチ（以下、ＯＦＳと記す）３とに分離されている。ＯＦＣ４は、ＯＦＳ３内のスイッチ３２へのパケット入出力処理動作やセキュリティ機能の制御を行う。ＯＦＳ３は、スイッチ３２と、フローテーブル３１を備える。スイッチ３２は、ＯＦＣ４の指示に従い、入力トラヒックのパケットデータのフラグ情報に基づいて、パケットに対するルーティングの処理（アクション）や暗号化等の符号処理を行う。

【００４０】

ネットワーク管理者は、入力トラヒックのパケットに付与されたフラグ情報の種別により、セキュリティ機能を規定し、当該パケットの暗号化、分割化、シャフリング等の秘匿化方法および、経路設定方法等のアクションを、事前に、フローテーブル３１内のフローエントリーにインストラクションとして登録する。このフローエントリー内のインストラクション等のパケット処理に関わる制御内容は、ＯＦＳ３の外部にあるＯＦＣ４からのソフトウェアにより管理される。ＯＦＳ３は登録されたフローテーブル３１に対して、パケットデータの処理に関わるマッチングルールを適用して、マッチしたフローエントリーに示された転送処理を当該パケットに対して行う。ＯＦＳ３は、自身のフローテーブル３１にて未定義のトラヒックフローが到着した場合、ＯＦＣ４に未定義フローに対する動作（アクション）を問い合わせる場合がある。ＯＦＣ４は未定義フローに対する動作を、当該ＯＦＳ３に指示する。ＯＦＳ３に入力されるパケット処理用のフラグに対して、予めフローテーブル３１（インストラクション等のアクションリスト）に未登録のパケット識別フラグがある場合には、ＯＦＳ３とＯＦＣ４との間で、制御メッセージのやり取りが発生する。

【００４１】

図６に示すＳＤＮにおけるネットワーク制御を考えた場合、ＯＦＣ４の位置する制御レイヤ６の下位は、インフラストラクチャーレイヤ５と位置付けるのが一般的である。この場合、レイヤ５の上位に、ＯＦＣ４を包含する制御レイヤ６があり、ＯＦＣ４の上位には、ネットワークアプリケーションレイヤ７を配備する方法が一般的である。この場合、ネットワークアプリケーションレイヤ７内の各種アプリケーション７１は、ＯＦＣ４の上位に存在し、新しいネットワーク制御用のアプリケーションソフトウエアを導入する場合や、ネットワーク制御用の経路計算アルゴリズムを変更する場合など、通常のネットワーク管理や監視機能を更改する場合などに活用する。ＳＤＮに関する標準化はＡＰＩも含め、まだ十分には進んでおらず、各ＯＦＣ４の実装に依存してアプリケーション７１も実装されているのが現状である。本発明における記述では、既存のＯＦＣ４とアプリケーションが１つの物理または仮想マシン上に実装されている場合において、クラウドの等の仮想環境を活用することもできる。将来的にＯＦＣ４とアプリケーション７１間のＡＰＩが定まった場合は、最も適切なアプリケーションを適用することも実施形態として有効である。

【００４２】

図７にスイッチで、アクション用に指定可能な制御コマンドの例を示す。図８にオープンフローで定義可能なヘッダ情報の例を示す。ＯＦＳ３は、制御コマンドの格納されたアクションテーブルを備え、制御コマンドおよびヘッダ情報の種別を活用して、前記の一連の処理をネットワーク内のスイッチ３２に実装することにより、ユーザ端末１１がデータ

バックアップを目的とした暗号化通信を行う場合に必要となる処理負荷を軽減することができる。さらに、セキュアーな通信を、ＯＦＳ３及びＯＦＣ４というネットワーク内機器の制御のみで実現することが可能となる。

【００４３】

一方、本実施形態に係るネットワーク制御方法は、データ送信手順と、データ受信手順とを順に有する。

データ送信手順において、ユーザ端末１１からの通信データを受信したＯＦＳ３が、分割処理を行った後にシャッフリング処理を行うとともに、分割処理及びシャッフリング処理の情報を、ユーザ端末１１からの通信データのメタデータとしてＯＦＣ４に格納する。ここで、分割処理は通信データを複数の断片データに分割する処理をいい、シャッフリング処理は断片データの配列順を変更することをいう。分割処理の情報は、通信データをどのように分割したかの情報であり、例えば、各断片データのデータ量であったり、等分割するために必要となるパディング情報の容量の大きさ等である。シャッフリング処理の情報は、断片データの配列順をどのように変更したかの情報である。

データ受信手順においては、ＯＦＳ３又はユーザ端末１１が、ＯＦＣ４に格納されているメタデータに従って断片データを配列しなおす。これにより、ユーザ端末１１から元の通信データに復元する。

【００４４】

データ送信手順では、ＯＦＳ３が、ユーザ端末１１からの通信データを符号化して通信データを複数の断片データに分割するか、或いはユーザ端末１１からの通信データを複数の断片データに分割して各断片データを符号化することが好ましい。この場合ＯＦＳ３で行った符号化処理をされたデータを復号化するために必要なデータをメタデータとしてＯＦＣ４に格納する。

【００４５】

図９に、本実施形態に係る受信手順における第１のシーケンスを示す。

ＯＦＳ３は、断片データを受信すると、受信データがある旨の受信メッセージを、宛先のユーザ端末１１に通知する。

ユーザ端末１１が通信データを受信する際には、まず、ユーザ端末１１はＯＦＳ３からの認証を受ける。例えば、ユーザ端末１１がＯＦＳ３へ認証要求を行い、ＯＦＳ３がＯＦＣ４に格納されている認証情報に基づいてユーザ端末１１の認証を行うことが好ましい。

ＯＦＳ３は、ユーザ端末１１の認証の完了後にデータの復元要求メッセージをユーザ端末１１から受信すると、ＯＦＣ４に格納されているメタデータを用いて断片データを元の通信データに復元し、ユーザ端末１１へ送信する。このとき、ＯＦＳ３がユーザ端末１１からの通信データを符号化している場合は、断片データの再配列と共に復号化も行う。

これにより、ユーザ端末１１は復元した通信データを受信する。また、宛先となるユーザ端末が認証を要求されないで、復元した通信データをＯＦＳから受信できる通信手順も同様に可能であることは言うまでもない。

【００４６】

図１０に、本実施形態に係る受信手順における第２のシーケンスを示す。

ＯＦＳ３は断片データを受信すると、断片データを宛先のユーザ端末１１に送信する。

ユーザ端末１１が元の通信データを受信する際には、まず、ユーザ端末１１はＯＦＳ３からの認証を受ける。ＯＦＳ３は、ユーザ端末１１の認証の完了後にデータの復元要求メッセージをユーザ端末１１から受信すると、ＯＦＣ４に格納されているメタデータを取得し、ユーザ端末１１へ送信する。

ユーザ端末１１は、メタデータを用いて断片データを元の通信データに復元する。このとき、ＯＦＳ３がユーザ端末１１からの元の通信データを符号化している場合は、当該メタデータを用いて、断片データの再配列化と共に復号化を行うことも可能である。

【００４７】

このように、本実施形態に係る発明は、図１１に示すように、ユーザ端末は、暗号化等

に関わる処理には関与せず、これらはネットワーク内のＯＦＳ３とＯＦＣ４を用いることにより、図３、図４に示す通信シーケンスに比べ、大幅にオーバヘッドを削減して、その分だけユーザ端末の通信スループットを向上できる。したがって、本実施形態に係るシステムは、ホスト側ではセキュリティ機能向上のための暗号処理等を、一切行うこと無く、代わりにＳＤＮ内のスイッチおよびコントローラが共同して、セキュリティ上の保証を行う安全配信（通信）の実現メカニズムを提供することができる。

【００４８】

（実施形態２）

本実施形態に係る発明は、ユーザ端末１１のファイルバックアップにも適用可能である。具体的には、ユーザ端末１１からＳＤＮ内のスイッチ（ＯＦＳ３）へ送られたファイルバックアップのための、ユーザ要求パケットデータに含まれる、フラグ種別情報により、対応するアクションテーブルがアクセスされる。アクションテーブル内の情報に基づいて、スイッチは当該のセキュリティを確保するために、各種の符号化処理（暗号化処理等を含む）を実施し、その後、スイッチ内で分割、シャッフリング及び複製処理を行い、目的の出側方路の先にあるストレージへ格納することにより、第３者によるデータの盗聴時の解読性を困難にすることができる。すなわち、ホスト－ストレージ間やホスト－サーバ間の通信において、ＳＤＮのスイッチが自律的に暗号化を行うことが可能になる。

【００４９】

端末側もしくはサーバ側の通信端末ではなく、通信ノード内のスイッチで暗号化・復号化を行うため、ホストまたはサーバが、暗号化または復号化に使用する鍵を管理する必要はなくなり、利便性の向上と安全性の向上の双方を同時に実現できる。この理由は、スイッチやコントローラが当該の符号化処理アルゴリズムの実行に必要な鍵を管理することにより、悪意のある第３者に対する機密性を高めることができるからである。一般的に、ユーザ端末や、サーバに比べて、ＯＦＣ４、ＯＦＳ３等のネットワーク内の制御装置や通信ノードは、外部からのアクセスが困難であり、これらのネットワーク機器に対する制御は、通常はインターネットから分離して運用されることが前提となるからである。一方、ユーザ端末１１やサーバはメール送信やインターネットを含めた外部へのサービス公開を行うことが多く、遠隔制御用プログラムの稼働や、不特定多数のユーザ端末との直接的なデータ通信の機会があるため、不正アクセス等により、安全性が損なわれる可能性が高い。

【００５０】

具体的には、サービスを利用するユーザ端末１１は、バックアップ要求メッセージをＯＦＳ３に送信する。ＯＦＳ３は、認証処理後にバックアップ対象となる元の通信データを符号化処理を行い、その後、メタデータをＯＦＣ４に格納する。その後、宛先に対応するストレージに送信する。ＯＦＣ３は、以後、復元要求があった場合は、ＯＦＣ４に格納されたメタデータを回収し、これを使用することにより、復号処理を行うことができる。

【００５１】

なお、ユーザ端末１１が故障等が生じたことにより、バックアップされた断片データの回収ができなくなった場合には、別のユーザ端末１１を使用し、適切な認証手順を経て、バックアップ先からの断片データの回収を実現することが可能となる。悪意あるユーザによって、不正にデータを復元されることを防ぐために、元の通信データに復元する際には、認証が必要であることは言うまでもない。認証方式はどのような方式を用いても構わない。以下に、チャレンジレスポンス方式による処理フローの一例を図１２に示す。

【００５２】

ユーザ端末１１は、認証要求メッセージをＯＦＳ３に送信する。ＯＦＳ３は受信した認証要求メッセージをＯＦＣ４に転送する。認証要求メッセージを受信したＯＦＣ４は、チャレンジと呼ばれるランダムな値を生成し、ＯＦＳ３に送信する。ＯＦＳ３はチャレンジをユーザ端末１１に転送する。

ユーザ端末１１は、受信したチャレンジと、認証に必要な情報で、レスポンスと呼ばれるハッシュ値を生成し、レスポンスをＯＦＳ３に送信する。ここで必要な情報は、ユーザＩＤとパスワードを含むことが好ましい。この場合、ユーザＩＤとパスワードは、事前に

ＯＦＣ４の認証データベースに保存しておくことが好ましい。ＯＦＳ３はレスポンスをＯＦＣ４に転送する。

レスポンスを受信したＯＦＣ４は、ユーザ端末１１と同様に送信したチャレンジと、ユーザＩＤとパスワードから、照合用のレスポンスを生成し、受信したレスポンスと生成したレスポンスとのバイナリコードを比較し、これらが一致すれば、認証が成功した旨を伝えるべく、認証応答を返送する。一致しない場合には、その旨（認証が失敗した旨）を伝える認証応答を返送する。

【００５３】

認証が成功した場合、ユーザ端末１１は、復元要求メッセージをＯＦＳ３に送信する。認証が成功した後の、ユーザ端末１１とＯＦＳ３、ＯＦＣ４の間の通信シーケンスをまとめて図１３に示す。図１３にはＯＦＳ３とＯＦＣ４の間およびＯＦＳ３とストレージ１２の間におけるハッシュ値の照合を併せて示す。

ＯＦＳ３は、認証が成功したユーザ端末１１からの復元要求メッセージの場合には、メタデータの問い合わせをＯＦＣ４に対して行う。ＯＦＳ３は、ＯＦＣ４からハッシュ付きのメタデータを回収し、データのハッシュ値の照合が完了した後に、ストレージ１２宛に、断片データの回収を行うための送信要求を送信する。なお、ユーザ端末１１からの認証要求における認証が失敗した場合には、ＯＦＳ３はユーザ端末１１からの復元要求メッセージのパケットを破棄する。

ストレージ１２は復号フラグを含んだヘッダ情報と保存された断片データのハッシュ値を付加したデータをＯＦＳ３に送信する。ＯＦＳ３は、ストレージ１２から受信したハッシュ値の照合を行い、メタデータをもとに復号処理を行い、復号後の元の通信データをユーザ端末１１に送信する。

以上述べた手順により、ユーザ端末１１が要求した、ストレージ１２にバックアップされた断片データは、ＯＦＳ３によって復号され、ユーザ端末１１で回収できる。

【００５４】

（実施形態３）

実施形態１の通信システムにおける第１の形態例を図１４に示す。第１の実施形態はサービスを利用するユーザ端末１１、ストレージ１２、オープンフロースイッチ（ＯＦＳ）３、及びオープンフローコントローラ（ＯＦＣ）４を備える。ユーザ端末１１は、サーバや、パーソナルコンピュータ、携帯端末などの重要データを保持し、記憶デバイスの故障や災害などの危険に遭遇する可能性がある。ストレージ１２は、ネットワーク上のユーザ端末１１からアクセス可能なデバイスである。例えば、ＮＡＳ（Ｎｅｔｗｏｒｋ　Ａｔｔａｃｈｅｄ　Ｓｔｏｒａｇｅ）やファイルサーバ、クラウドストレージなどが該当する。

【００５５】

ＯＦＳ３はサービス利用端末１１及びストレージ１２の間のコネクションを確立するためのスイッチを含む通信ノードであり、通常のＯＦＳにおける目的方路へのルーティングの機能に加え、本発明で開示した、暗号化等を含む符号化処理と復号化処理の機能を実装している。ＯＦＳ３は、ファイルのバックアップ処理等の通信サービスを実施するため、ユーザ端末１１から、バックアップしたい通信データを受け取った場合は、当該の符号化処理を行い、ストレージ１２に格納する。ユーザ端末１１から復元要求があった場合には、ストレージ１２との接続を行い、その後、必要なファイルを読み出し後に、ＯＦＳ３で復号処理を行い、当該ユーザ端末１１に復元結果を転送する。

【００５６】

ＯＦＣ４は、ＯＦＳ３を管理するコントローラであり、ストレージ１２とコネクションを確立する。ＯＦＣ４はＯＦＳ３からバックアップ要求のメッセージを受信後、ＯＦＳ３での符号化に必要となる、アクションテーブルに格納する情報をＯＦＳ３に返送する。この情報は、例えばストレージ１２はどのポートと接続されているかや、符号化・復号化の処理に必要となる暗号化用パラメータなどを含む。

【００５７】

通信ネットワーク２１、２２、５は通信可能な情報伝達網であり、例えばＬＡＮ（Ｌｏ

ｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）も含まれる。通信ネットワーク５は、ＯＦＣ４が、ＯＦＳ３を制御する通信のみに用いる。本実施形態の例では、通信ネットワーク５は、ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）通信又はＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）暗号通信を用いたものであることが好ましい。本実施形態の例では、データセンタ内で適用する例について説明するが、この例に限らず、インターネットを含めた各種ネットワークにも部分的に適用可能である。

【００５８】

ユーザ端末１１は、バックアップしたいデータファイルをＵＤＰ／ＩＰを用いて、ストレージ１２に格納することが好ましい。例えば伝送回線の品質が高い場合にはＵＤＰを用いる場合が適しているが、この方法に限定されるものではなく、例えば、ホスト間の通信にＴＣＰを用いて実施することも可能である。ユーザ端末１１は、バックアップしたいデータを、ストレージ１２に送信するために、ＩＰヘッダおよびＵＤＰヘッダ（あるいはＴＣＰヘッダ）を付加するが、同時に、ネットワーク内のスイッチでの、セキュアーなバックアップサービスの実現に対応した符号化処理用のフラグ情報をヘッダ内に記載する必要がある。スイッチ内における、バックアップ対象となるデータファイルの処理形態は、ユーザが要求するセキュリティの重要度に基づいて、フラグ情報種別を変更することにより、対処が可能である。例えば、セキュリティの重要度の低いデータファイルは、暗号化せずに平文のまま送信し、セキュリティ上の重要度の高いデータファイルであれば、送信前にＡＥＳ等で、暗号化してからファイルを送信することも可能である。セキュリティレベルの詳細については、特許文献１に開示されている。

【００５９】

図１５は本実施形態における第２の形態例を示しており、ユーザ端末１１が１１ａから１１ｂの全てを含む場合を想定している。この１１ａから１１ｂの中の一つから、復元要求がある場合に、当該ユーザ端末とストレージ１２との接続を行い、その後、必要なファイルは、１１ａから１１ｂのどれからでも読み出しできる場合のシステム構成例を示している。

ＯＦＳでの復号処理や、当該ユーザ端末に復元結果を転送する方法は、実施形態１の場合と同様である。

【００６０】

（実施形態４）

実施形態２の通信システムに係る第１の形態例を図１６に示す。本実施形態ではストレージ１２が１２ａからストレージ１２ｄの４つのストレージから構成される例を示す。ＯＦＣ３の処理フローは、後述する図１８のステップＳ１０９において、ヘッダ情報を付加して送信する際に、ストレージ１２ａ～１２ｄの４つのストレージに同一パケットを、複製して送信することが、オープンフローを用いて実装可能である。ＯＦＣ４からは、ｐａｃｋｅｔ＿ｏｕｔメッセージ内にストレージ１２ａ～１２ｄが接続されているポートに対し、パケットを送出するように指示をすることで実現できる。

【００６１】

また復元処理の際には、ＯＦＳ３が、ＯＦＣ４から受信したメタデータから、ストレージ１２ａ～１２ｄに対して、データの送信要求を送出し、どれか一つのストレージから断片データが受信できた場合には、復号処理を開始し、復号結果の元の通信データをユーザ端末１１に送信する。ストレージ１２ａ～１２ｄに対し、同じように符号化された冗長データをバックアップすることにより、信頼性を高めることができる。ストレージ１２ａ～１２ｄのうちのどれか一つが稼働していれば、復元が可能となるからである。

【００６２】

上記の冗長化の例では、ストレージ端末の耐障害性を高めることができるが、分散方法を工夫することにより、セキュリティ強度を高めることも可能である。例えば、暗号化したデータの半分を、ストレージ１２ａ、１２ｂに、もう半分をストレージ１２ｃ、１２ｄにバックアップするようにｐａｃｋｅｔ＿ｏｕｔメッセージを用いて、対応するパラメータ設定を行うことにより、ストレージ１２ａか１２ｂのどちらかが正常であり、かつスト

レージ１２ｃか１２ｄのどちらかが正常である場合に限って復元することができる。この場合、ストレージ１２ａと１２ｂのみでは復元できないため、悪意あるユーザにより、ストレージ１２ａか１２ｂのどちらがハッキングされ、かつ、ストレージ１２ｃか１２ｄのどちらかがハッキングされる条件が揃わない場合以外は、元の通信データの復元は不可能となる。この場合、ＯＦＳの中にバッファリングされるパケットデータは、２分割され、それぞれが別のストレージに格納される。この例の他に、セキュリティのレベルに応じて適切に分割数を大きくとることも同様に可能であることは言うまでもない。

【００６３】

上記の一連の実施形態において、使用されるフラグ情報の記載方法を図１７に示す。図１７にはＩＰヘッダのオプション領域を使用して、符号化処理を行うフラグ種別、復号処理を行うフラグ種別、符号化、復号処理共に、必要のない、通常のパケット処理を行うフラグの３種類のフラグ情報のどれかを記載することにより、セキュリティ機能の異なる通信サービスの要求を実現できる。ＩＰヘッダ長は４の倍数バイト長になるためオプション領域は４バイトとなる。スイッチ内において符号化処理を行う必要のあるパケットに関しては、例えばオプション領域のビット列を、０ｘ８０００００００とする。復号処理が必要なパケットは、０ｘ４０００００００とする。符号化、復号処理の必要ない通常のパケットは、０ｘ００００００００もしくは、オプション領域がないものとする。このように、ＩＰヘッダのオプション領域を用い、３種類のパケットを識別するが、この方式に限定されるものではない。例えば、高いセキュリティのレベルのバックアップを実現したい場合には、そのレベル種別数に応じてフラグ種別を設けることで対処が可能である。各種のセキュリティレベルの内容の例に関しては、特許文献１に開示された技術が対象となる。ユーザ端末１１は、ストレージ１２に送信する際に、上述したＩＰヘッダのオプション領域に０ｘ８０００００００を設定する。その他のヘッダ情報は、通常のＵＤＰ／ＩＰを用いた通信と同様に設定する。この場合のＯＦＳ３の処理フローを、図１８に示す。

【００６４】

パケットを受信したＯＦＳ３（ステップＳ１０１）は、ヘッダ内容を解析し、符号化処理を行うパケットか、または復号処理を行うパケットか、または通常のパケットか、を上記のＩＰヘッダのオプションのフラグで識別する（ステップＳ１０２）。通常のパケットの場合は通常の処理Ｓ１０３を行い、パケットを送出する（ステップＳ１０３）。符号化処理が必要な場合はステップＳ１０４～Ｓ１１０を行い、復号処理が必要な場合はステップＳ１１１～Ｓ１１７を行う。

【００６５】

ステップＳ１０３では、例えば、ルーティング処理やフォワーディング処理を行う。

ステップＳ１０４ではメタデータを読み込み、ステップＳ１０５ではバッファ処理を行い、ステップＳ１０６では符号化処理を行い、ステップＳ１０７では分割処理を行い、ステップＳ１０８ではシャッフリング処理を行い、ステップＳ１０９ではヘッダを付加してパケットを送信し、ステップＳ１１０では復号化に必要なメタデータをＯＦＣ４へ送信する。

ステップＳ１１１では当該のメタデータを読み込み、ステップＳ１１２ではバッファ処理を行い、ステップＳ１１３ではシャッフリングされた順番を元に戻し、ステップＳ１１４では復号処理を行い、ステップＳ１１５では分割処理を行い、ステップＳ１１６ではヘッダを付加してパケットを送信し、ステップＳ１１７では復号の完了をＯＦＣ４に知らせる。

【００６６】

符号化処理の場合（Ｓ１０４～Ｓ１１０）、符号化処理を行うための各種パラメータ（以後、メタデータと呼称する）を、未設定であることが判断された場合は、ＯＦＣ４に問い合わせる。ＯＦＳ３とＯＦＣ４の間のメタデータ問い合わせ手順に関する具体的な通信シーケンスを図１９に示す。ＯＦＳ３は未知のパケットが届くと、ＯＦＣ４にｐａｃｋｅｔ＿ｉｎメッセージと呼ばれる未知のパケットのヘッダ情報等をＯＦＣ４に問い合わせる。ｐａｃｋｅｔ＿ｉｎメッセージを受け取ったＯＦＣ４は、受け取った情報をもとに、Ｏ

ＦＳ３にメッセージを返送し、未知のパケットの操作を指示し、ＯＦＳ３はフローテーブル３１に指示された操作に従って当該未知のパケットの設定を行う。例えば、パケットを特定のポートから送出する操作をＯＦＣ４が指示する場合、ＯＦＣ４はｐａｃｋｅｔ＿ｏｕｔメッセージをＯＦＳ３に送る。ＯＦＳ３が持つフローテーブル３１に情報を追加する操作をＯＦＣ４が指示する場合は、ｆｌｏｗ＿ｍｏｄメッセージを併せてＯＦＳ３に送る。

【００６７】

本実施形態では、上記のＯＦＳ３、ＯＦＣ４のやりとりに、符号化、復号化に必要なメタデータを送受信するメッセージを定義する必要がある。パケットを受信したＯＦＳ３は、ｐａｃｋｅｔ＿ｉｎメッセージとメタデータの問い合わせをＯＦＣ４に行う。ｐａｃｋｅｔ＿ｉｎメッセージとメタデータの問い合わせを受信したＯＦＣ４は、ルーティングの決定や、送出先のポートの決定などの、従来のルータ処理に加え、設定すべきメタデータをＯＦＳ３に送る。ＯＦＳ３は受け取った情報をもとに、バッファ処理、符号化処理、分割処理、シャッフリング処理、パケットの送出処理を行い（ステップＳ１０５～Ｓ１０９）、復号処理に必要となるメタデータをＯＦＣ４に送信する。ＯＦＣ４は受信したメタデータを復号処理が行われるまで保持する。

【００６８】

バッファ処理時（ステップＳ１０５）及び符号化処理（ステップＳ１０６）のフローの一例を、図２０、図２１に示す。メタデータに設定されたパラメータ変数を取り出す（Ｓ２０１）。パラメータ変数には、符号化処理用のバッファに格納されたパケット数Ｎ、バッファするパケット数Ｍ、ＭＳＳ（Ｍａｘｉｍｕｍ　Ｓｅｇｍｅｎｔ　Ｓｉｚｅ）、タイムアウト設定時間Ｔ等が存在する。ＭＳＳに関しては、通信ネットワーク上で、ＩＰフラグメンテーションを起こさないための最大ペイロード長を指定することが好ましい。

パケットからＵＤＰペイロードを取り出し、符号化処理用のバッファにバッファリングする（Ｓ２０４）。符号化処理のバッファにＭ個のパケットをバッファリングした後、バッファリングしたデータサイズがＭＳＳ×Ｍサイズ未満だった場合、ＭＳＳ×Ｍサイズにパディング処理を行い（Ｓ２０９）、図２１に示す符号化処理においてＭＳＳ×Ｍサイズに合わせた後で当該データを符号化処理する。ここでパディング処理でパディングするビット列は、乱数列であることが好ましい。

また、次のパケットを受信するまでに、タイムアウト設定時間Ｔが過ぎた場合（Ｓ２０８においてｎｏ）、上記と同様にパディング処理を行い（Ｓ２０９）、図２１に示す符号化処理を行う。タイムアウト規定を設ける理由は、パケットがこれ以上のパケットの受信が生じないと推定される場合や、一定の遅延時間を超える状況が発生した場合には、バッファリングしているパケットが、ＯＦＳ３からまとめて送出されない可能性があるからである。

【００６９】

以上の処理を繰り返し、到着パケットに対して、ＯＦＳ３はステップＳ１０５のバッファリングを行う。例えば、最も簡単な一例として、Ｍ＝３、ＭＳＳ＝１４７２、Ｔ＝１ｍｓとした場合、パケットを３個分まで、バッファリングする。符号化処理用のバッファに格納されたパケット数Ｎが、３になるまでＯＦＳ３はバッファリングし（Ｓ１０５）、符号化処理を行う。ただし、２個のパケットを受信した後、３個目のパケットを受信するまでに、１ｍｓ以上の時間がかかった場合、３個目のパケット分のサイズになるまで、ＯＦＳ３がパディングして符号化処理を行う。

【００７０】

図１８に示す符号化処理（ステップＳ１０６）は、上記のバッファ処理で、符号化処理用バッファにバッファリングされた通信データに符号化を行う。例えば、ランダムなビット列とのＥＸＯＲ演算を行った後に、一体化と呼ばれる可逆演算（特許文献２で開示）によって撹拌することにより、ビット列をランダムな形態にする。具体的な符号化処理フローの実施形態を図２１に示す。

【００７１】

先ず、受信した通信データに対してランダムなビット列とのＥＸＯＲ演算処理（ステップＳ３００）を行い、以降で使用する符号化処理用のデータを初期設定する。
次に、バッファリングされた通信データを、４バイトごとにｘ（０）、ｘ（１）、…、ｘ（ｎ）とする（ステップＳ３０１）。インデックスｉ＝０とし、ｘ（ｉ＋１）＝ｘ（ｉ＋１）＋ｘ（ｉ）を、ｉ＜ｎまで繰り返す（ステップＳ３０２～Ｓ３０５）。
最後にｘ（０）＝ｘ（０）＋ｘ（ｎ）とする。

【００７２】

この符号化処理は予め定めた基準に従って複数回実施し、ビット列を撹拌することが好ましいが、機密性を確保するためには、この回数は適宜、変更することが、より好ましい。また、十分に撹拌処理を行うためには、符号化処理の回数は６回以上であることが好ましい。本実施形態では、加算演算により、元の通信データの撹拌を実施しているが、これは限定されるものではなく、可逆演算であれば、どのような演算種別を用いても良い。例えば、ステップＳ３０４、Ｓ３０６の演算を排他的論理和演算に変更して、実施しても良い。

【００７３】

符号化処理によって、撹拌されたデータを、１パケットのペイロードサイズ（ＭＳＳ）に分割を行う（ステップＳ１０７）ことが好ましい。バッファ処理において、ＭＳＳ×Ｍサイズにパディング処理を行っているため、撹拌されたデータは、Ｍ個でＭＳＳサイズのデータとなる。ＭＳＳサイズとするのは、通信ネットワーク上で、フラグメンテーションが発生しないようにするためである。

【００７４】

シャッフリング処理（ステップＳ１０８）は、上記の分割処理（ステップＳ１０７）において、分割されたＭ個の断片データをランダムな順番に、シャッフリングする処理である。具体的なシャッフリング処理フローの例を図２２に示す。シャッフリングは例えば、Ｆｉｓｈｅｒ－Ｙａｔｅｓアルゴリズムを用いることが、一様ランダムな配置形態が実現可能であることから、好ましい。Ｆｉｓｈｅｒ－Ｙａｔｅｓアルゴリズムでは、先ず、擬似乱数ｊを生成し、分割された断片データをステップＳ５０２～Ｓ５０６の処理を行うことにより、一様ランダムな順番にシャッフリングを行うことができるためである。擬似乱数ｊは、どのような擬似乱数生成を用いてもよいが、真正乱数に近く、推測されにくいアルゴリズムが好ましい。

【００７５】

以上述べたバッファ処理、符号化処理、分割処理、シャッフリング処理（ステップＳ１０５～Ｓ１０８）を行うことで、元の通信データに暗号化処理を行うことができる。Ｍ個のデータを一つのデータとみなして全体の撹拌を行い、撹拌されたデータをＭ個に分割し、順番をランダムに並び替えることができる。悪意ある第３者が復号する場合には、Ｍ個の断片データを全て集め、正しい順番に並び替え、復号を行わなければならない（特許文献１で開示）。

【００７６】

一般にＭを十分大きな数に設定した場合には、全ての断片データを集めたることに加え、更に、元の順番に並び替えるためには、Ｍ！通りの組み合わせを総当たりで試す必要がある。このため、Ｍの値が４０を超える程度の分割であれば、解読処理量の面からは、計算量的な安全性を十分に確保できると考えられる。なお、スイッチはシャッフリングされた順番に従い、パケットデータに当該ヘッダ情報を付加して送信するが、このパケットデータに付加するヘッダ情報は、受信端末のネットワーク環境を考慮し、ネットワーク装置特有のパラメータに整合させる必要がある。例えばＬ２スイッチとして使う場合は、送信元、送信先ＭＡＣアドレスへの付け替えが必要であり、ＭＡＣヘッダ内のＦＣＳを変更する必要がある。Ｌ３スイッチとして使用する場合には、上記の変更に加え、ＩＰアドレス情報の書き換えなどが必要である。なお、本発明ではパケットの順番を表すヘッダ情報（例えばＩＰヘッダのフラグメントオフセットやＴＣＰヘッダのシーケンス番号など）は、受信時のヘッダ情報に記された順番ではなく、シャッフリングされた後の順番を記載する

必要がある。
【００７７】
復号化に必要なメタデータはＯＦＳ３からＯＦＣ４へ送信する（ステップＳ１１０）。復号化に必要なデータ種別には、バッファ処理の際に必要になるＭＳＳサイズ、バッファするパケット数Ｍが含まれる。復号化を実施する場合には、符号化に用いた逆関数、シャッフリング前の順番とシャッフリング後の順番などの情報が必要である。これらの情報を含むメタデータはＯＦＣ４に送信され、復号化が完了するまで保持される。ＯＦＣ４は他のデバイスとＶＰＮ等の専用網で接続され、インターネットには接続しない構成が好ましい。
【００７８】
本実施形態では、開示内容を明確化するため、メタデータに記載するパラメータを固定した単純な例を示したが、メタデータに記載する情報は、シャッフリング前後の順番に関するデータ以外は記載していないが、例えば、バッファするパケット数Ｍを動的に変化させることができ、この場合は符号化のたび毎にパラメータの変更値をメタデータとして保持する必要がある。
【００７９】
ＯＦＳ３が復号処理する際には、図１８のステップＳ１１１～Ｓ１１７に対応する処理の逆を行う。処理内容は、符号化の処理フロー手順（Ｓ１０４～Ｓ１１０）と逆向きの処理内容に対応する。すなわち、符号化処理によって、撹拌されたデータを、格納されたストレージから回収して、ＯＦＳ３のスイッチ内で復号化するには、撹拌に用いた関数の逆関数を実施する必要がある。図２０、図２１の符号化処理によって、撹拌されたデータを、復号化する具体的な処理を図２３に示す。
【００８０】
復号処理におけるステップＳ１１４は、図２３に示す逆関数処理を用いた復号処理に該当する。復号処理の完了後、ＯＦＳ３は復号化の完了通知をＯＦＣ４に送信し、ＯＦＣ４は関連するメタデータを削除する（ステップＳ１１７）。ステップＳ１１４における復号化時には、符号化処理と同様に、データを４バイトごとにｘ（０）、ｘ（１）、‥、ｘ（ｎ）とし（Ｓ４０１）、はじめにｘ（０）＝ｘ（０）＋ｘ（ｎ）を実行した後（Ｓ４０２）、ｘ（ｎ－１）＝ｘ（ｎ－１）＋ｘ（ｎ＋１）を繰り返す（Ｓ４０３～Ｓ４０６）。シャッフリングされたデータの順序を元に戻す処理や一体化処理の逆関数を用いることにより、復号処理が実施できる。
【００８１】
（実施形態５）
本実施形態に係る通信システムの形態例を図２４に示す。本実施形態における通信システムは、ユーザ端末１１、ストレージ６２～６７、オープンフロースイッチ（ＯＦＳ）７１、７２、７３及びオープンフローコントローラ（ＯＦＣ）８１、８２、８３から構成される。通信ネットワーク９１～９３は、例えば、ＬＡＮを使用し、９４は一般の公衆網の場合を想定して以下に説明する。通信ネットーク１０１～１０５は、ＯＦＣの制御用の通信網で、ＶＰＮ等の専用通信ネットワークであることが好ましい。
【００８２】
データセンタ１１１はＯＦＳ７２、ＯＦＣ８２、ストレージ６２～６４、データセンタ１１２はＯＦＳ７３、ＯＦＣ８３、ストレージ６５～６７を持つ。データセンタ１１１と１１２はそれぞれ地理的に離れた場所にある。実施形態３では、同じネットワーク内にストレージ１２ａ～１２ｄが存在したが、実用的には、ストレージ６２～６７をそれぞれ別のデータセンタ等、地理的に離れた場所に設置することにより、地震などの災害やハッキング等で、ストレージ６２～６７のすべてが同時に危険にさらされる事がないように構成できる。
【００８３】
本実施形態では、実施形態２における図１６においてＯＦＳ３が行った符号化処理と、複製・分散転送する処理を、それぞれ、符号化処理はＯＦＳ７１で行い、複製・分散転送

する処理はＯＦＳ７２と７３で、分担して実施する場合を示している。ここで、例えば、ＯＦＳ７２、７３は、符号化処理を行わずに複製および分散転送のみを行い、ストレージ６２～６４および６５～６７に分散転送する場合の例である。符号化処理や、復号処理、複製・分散転送する機能は、第３の実施形態と同様である。

【００８４】

メタデータは、ＯＦＣ８１～８３が、通信ネットワーク１０２、１０３を用いることで共有できる。従って、バックアップを行った際、ストレージ６２～６４はデータのハッシュ値をＯＦＣ８２に、ストレージ６５～６７はデータのハッシュ値をＯＦＣ８３に送り、ＯＦＣ８２、８３はＯＦＣ８１にハッシュ値を通知する。ＯＦＣ８１はメタデータに、ＯＦＣ８２、８３から受け取ったハッシュ値を記載する。

【００８５】

ユーザ端末１１が、復元要求をＯＦＳ７１へ行った場合、ＯＦＳ７１がＯＦＣ８１からメタデータを受信し、ＯＦＳ７２、７３にデータの送信要求を送る。ＯＦＳ７２、７３は、ストレージ６２～６４、および６５～６７に送信要求を送る。ＯＦＣ７１は、ストレージ６２～６４および６５～６７が返送したデータに対する復号処理を行い、復元データをユーザ端末１１に送信する。このように、ＯＦＳ７１で符号化及び復号化を行うことにより、仮に公衆網９４で第３者による盗聴があった場合でも、元データの復元は、関連するＯＦＣが保持するメタデータとＯＦＳで実施する復号処理メカニズムの詳細が不明である限り、不可能である。一般的には、処理負荷量のバランスを、ＯＦＳ同士でとることも可能であることは言うまでもない。

【００８６】

（実施形態６）

本実施形態に係る通信システムの形態例を図２５に示す。本実施形態に係る通信システムは、ユーザ端末１６１、１６２、オープンフロースイッチ（ＯＦＳ）１２１、１２２、およびオープンフローコントローラ（ＯＦＣ）１３１、１３２を備える。ユーザ端末１６１、ＯＦＳ１２１、ＯＦＣ１３１はデータセンタ１１１内に設置されており、ユーザ端末１６２、ＯＦＳ１２２、ＯＦＣ１３２はデータセンタ１１２内に設置されている。ユーザ端末１６１、１６２は、相互通信が可能な端末であり、ＯＦＳ１２１、１２２は、相互にコネクションを確立している。

【００８７】

ＯＦＳ１２１、１２２はエッジルータに対応し、データセンタ１１１とデータセンタ１１２との間でコネクションを確立しているノードである。ＯＦＣ１３１、ＯＦＣ１３２は、それぞれＯＦＳ１２１、１２２とコネクションを確立している制御ノードである。また、ＯＦＣ１３１、１３２は相互にコネクションを確立されている。通信ネットワーク１４１、１４２は、データセンタ１１１、１１２内のＬＡＮを想定するが、この形態に限るものではない。通信ネットワーク１４３は、公衆網である。

【００８８】

通信ネットワーク１５１、１５２は、それぞれ、ＯＦＣ１３１、１３２がＯＦＳ１２１、１２２を制御するための専用の通信ネットワークであり、ＶＰＮなどの専用通信ネットワークであることが好ましい。通信ネットワーク１５３は、ＯＦＣ１３１とＯＦＣ１３２間で、同期、制御を行うための専用の通信ネットワークであり、通信ネットワーク１５１、１５２と同様に、ＶＰＮなどの専用通信ネットワークであることが好ましい。通信ネットワーク１５３は、通信ネットワーク１５１、１５２と異なり、データセンタ１１１とデータセンタ１１２を相互接続する通信ネットワークであり、データセンタ内の通信ネットワーク１５１、１５２と同じように、セキュリティに配慮すべき専用ネットワークであることが好ましい。

【００８９】

本実施形態では、前述の実施形態１～実施形態３とは異なり、ユーザ端末１６１と１６２がデータ通信を相互に行うＰ２Ｐ通信を想定している。具体的には、ユーザ端末１６１が、ユーザ端末１６２に通信データを送信する際には、ＯＦＳ１２１が、図１８に示す符

号化処理に対応する処理を行う。この時、メタデータをＯＦＣ１３１から読み込み、バッファ処理、符号化処理、分割処理、シャッフリング処理およびパケットの送信処理を行い、当該のメタデータをＯＦＣ１３１に格納する。ＯＦＳ１２１で符号化処理されたパケットは、通信ネットワーク１４３を経由して、ＯＦＳ１２２に届く。

【００９０】

ここで、ＯＦＣ１３１はメタデータをＯＦＣ１３２に事前に送信し、ＯＦＳ１２２に対して提供する準備を行う。ＯＦＳ１２２は、ＯＦＳ１２１から受信したパケットに対して、図１８に示す復号処理を、ＯＦＣ１３２から受信したメタデータをもとに行い、ＯＦＳ１２１からの受信パケットをユーザ端末１６１が送信した符号化前のパケットに復号し、ユーザ端末１６２に送信する。その後、ＯＦＣ１３２には復号完了の通知を行う。

【００９１】

このように、ネットワーク内の機器であるＯＦＳ１２１で符号化し、ＯＦＳ１２２で復号することにより、公衆網である通信ネットワーク１４３で、仮に盗聴されたとしても、元の通信データを復元は非常に困難であり、第３者には解読困難な、秘密通信を実現できる。

【００９２】

ユーザ端末１６２がユーザ端末１６１に対して送信を行う場合は、上記とは逆の順番で、ＯＦＣ１３２、１３１が起動する。具体的には、ＯＦＳ１２２が符号化処理を行い、ＯＦＳ１２１が復号処理を行い、ＯＦＣ１３２がメタデータをＯＦＣ１３１に送信する。ＯＦＳ１２１と１２２が行う符号化、復号化の処理は、前述の実施形態１から実施形態３と同等であるが、バックアップサービスのように、ストレージから、断片データを回収するための手順が省略されている点が異なる。また、一般的には、ユーザ端末１６２は、認証手順を用い、照合が確認された段階で、ＯＦＳ１２２で復号化された通信データを受信することが好ましい。

【００９３】

以上、説明したように、本発明の特徴は、集中制御を前提とした、ＳＤＮのアーキテクチャを持つネットワーク制御方式において、

（１）ネットワークを集中制御するコントローラとスイッチの制御機構の活用により、ユーザ端末、あるいはサーバ側の制御とは独立に、高いセキュリティの通信を実現する。

（２）ユーザ端末の処理能力を暗号化処理等のために費やすことが無いため、容易に通信スループットの向上化が図れる。

（３）ＳＤＮ内の専用ネットワークと公衆網の適切な適用により、従来の通信方式に比べて、高いセキュリティを確保できる。

（４）トラヒックの急激な増加やネットワーク機器の故障等の状況に応じて、安全なバックアップサービスが容易に実現できる。

（５）端末同士の通信を、リアルタイムに、秘密通信として実現できる。

【００９４】

すなわち、開示した技術は、ＳＤＮのアーキテクチャをもつオープンフロースイッチとコントローラを活用することにより、安全でセキュリティの高い通信を実現すると共に、ユーザ端末であるホスト側の処理負荷の増大を一切起こすことなく、セキュリティ強度の高い暗号通信をネットワーク内のみで実現できるため、通信スループットの大幅な向上が期待できる。

【００９５】

本技術は、ＳＤＮに代表されるオープンフロータイプのネットワークに適用できるだけでなく、ＮＧＮや既存の携帯電話網の制御やオペレーションシステムの制御を行う場合にも適用でき、適用対象範囲は極めて広い。以上説明したように、本技術は、安全で高速なネットワークサービスを実現する上での基盤技術として活用でき、今後の情報通信産業を発展させる上で極めて大きな意義を持つ。

【産業上の利用可能性】

【００９６】

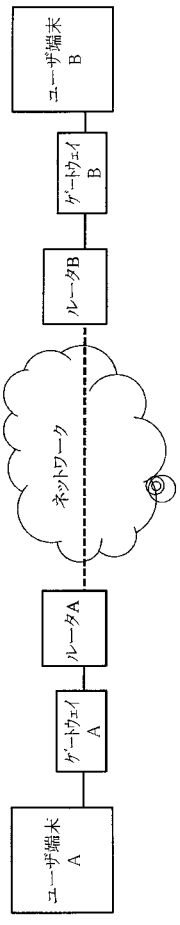
本発明は情報通信産業に適用することができる。

【符号の説明】

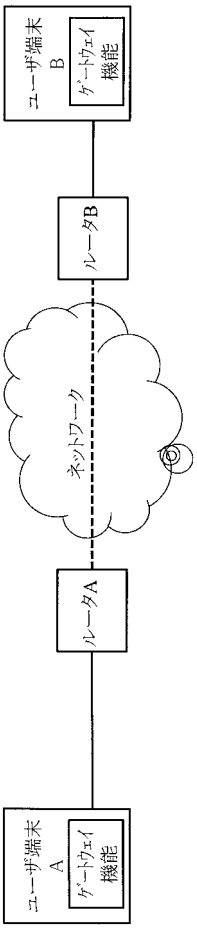
【００９７】

１１、１６１、１６２　ユーザ端末
１２　ストレージ
２１、２２　データ通信用ネットワーク
３、７１～７３、１２１、１２２　オープンフロースイッチ（ＯＦＳ）
３１　フローテーブル
３２　スイッチ
４、８１～８３、１３１、１３２　オープンフローコントローラ（ＯＦＣ）
５、１０１～１０５、１５１～１５３　制御用の専用通信ネットワーク
９１～９４、１４１～１４３　データ通信用ネットワーク
１１１、１１２　データセンタ（あるいはサービス利用端末）

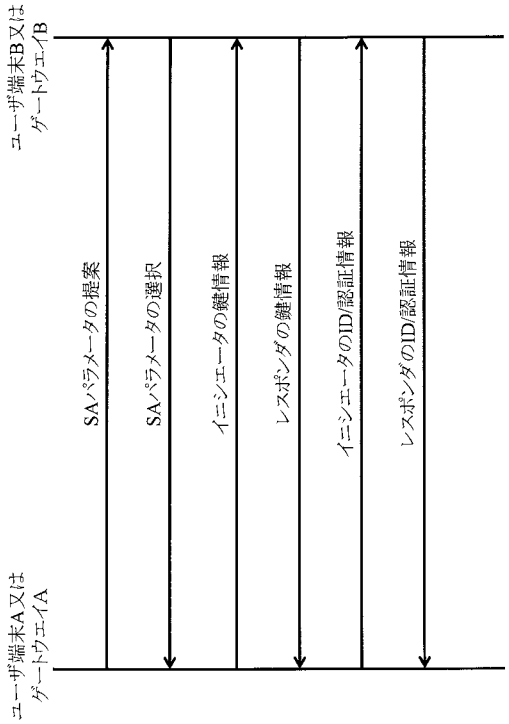
【図１】



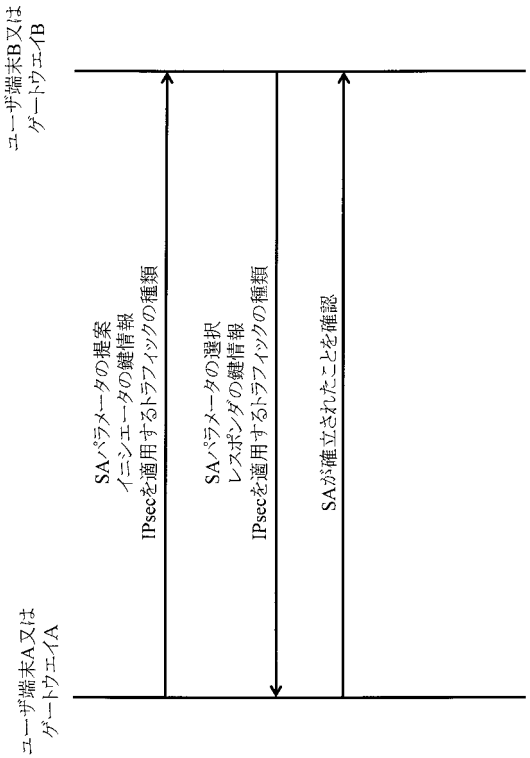
【図２】



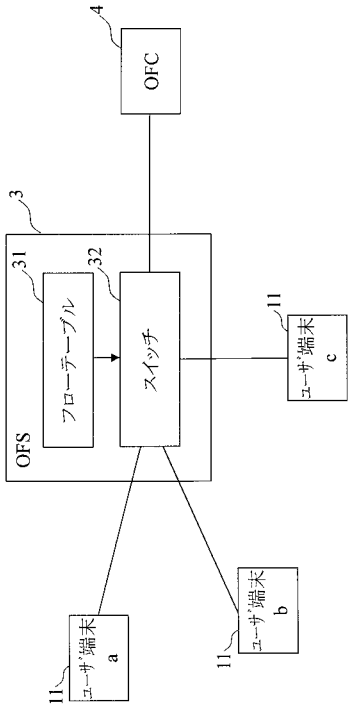
【図３】


ユーザ端末B又は
ゲートウェイB
ユーザ端末A又は
ゲートウェイA
SAパラメータの提案
SAパラメータの選択
イニシエータの鍵情報
レスポンダの鍵情報
イニシエータのID/認証情報
レスポンダのID/認証情報

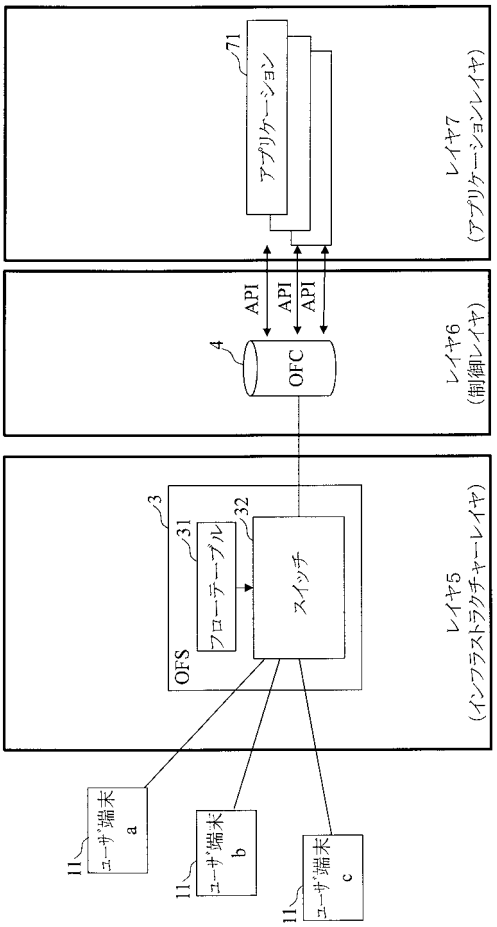
【図４】


ユーザ端末B又は
ゲートウェイB
ユーザ端末A又は
ゲートウェイA
SAパラメータの提案
イニシエータの鍵情報
IPsecを適用するトラフィックの種類
SAパラメータの選択
レスポンダの鍵情報
IPsecを適用するトラフィックの種類
SAが確立されたことを確認

【図５】


4
OFC
3
31
32
OFS
フローテーブル
スイッチ
11
ユーザ端末
c
11
ユーザ端末
a
11
ユーザ端末
b

【図６】


71
アプリケーション
レイヤ7
(アプリケーションレイヤ)
API
API
API
4
OFC
レイヤ6
(制御レイヤ)
3
31
32
OFS
フローテーブル
スイッチ
レイヤ5
(インフラストラクチャーレイヤ)
11
ユーザ端末
a
11
ユーザ端末
b
11
ユーザ端末
c

【図７】

制御コマンド

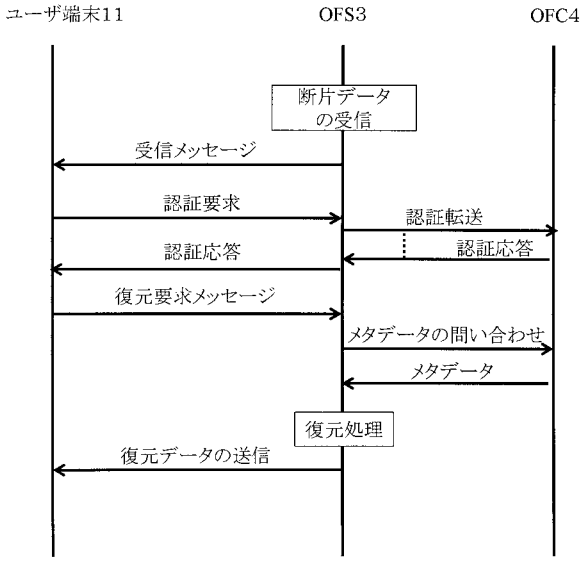
値	説明
Forward	パケットを特定の物理ポートに転送する
Drop	パケットを破棄する
Modify-Field	パケットヘッダの値を指定した値に書き換える
store	パケットを一時、格納する
copy	パケットをコピーし、複数ポートにマルチキャストする。
divide	パケットを分割し、複数ポートにマルチキャストする。
Encyption-A	パケットの中身をAESで暗号化する。
Encyption-S	パケットの中身を一体化処理(空間的に攪拌)する。

【図８】

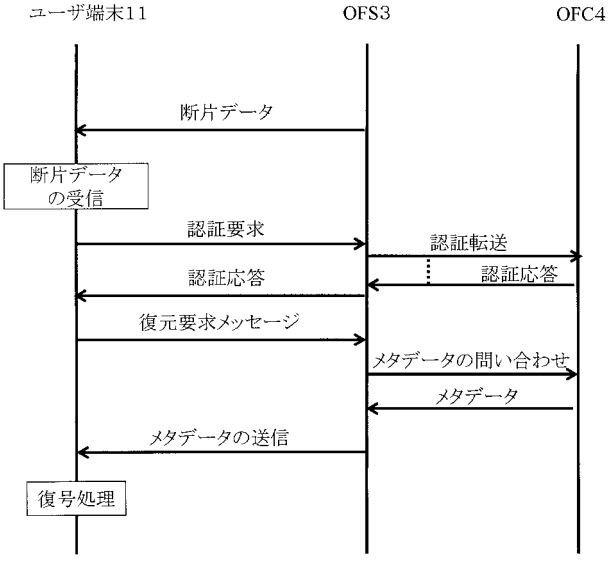
ヘッダ情報

No	ヘッダフィールドに指定可能な条件
1	物理ポート番号
2	送信元MACアドレス
3	送信先MACアドレス
4	Etherタイプ
5	VLAN ID
6	VLAN プライオリティ
7	送信元IPアドレス
8	送信先IPアドレス
9	IPプロトコル種別
10	IP TOS情報
11	送信元L4ポート番号
12	送信先L4ポート番号
13	MPLSラベル番号
14	閉域サービス識別番号
15	ファイルバックアップ用のセキュリティ番号

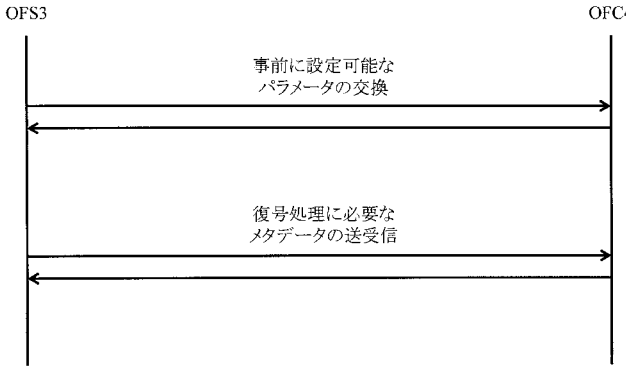
【図９】



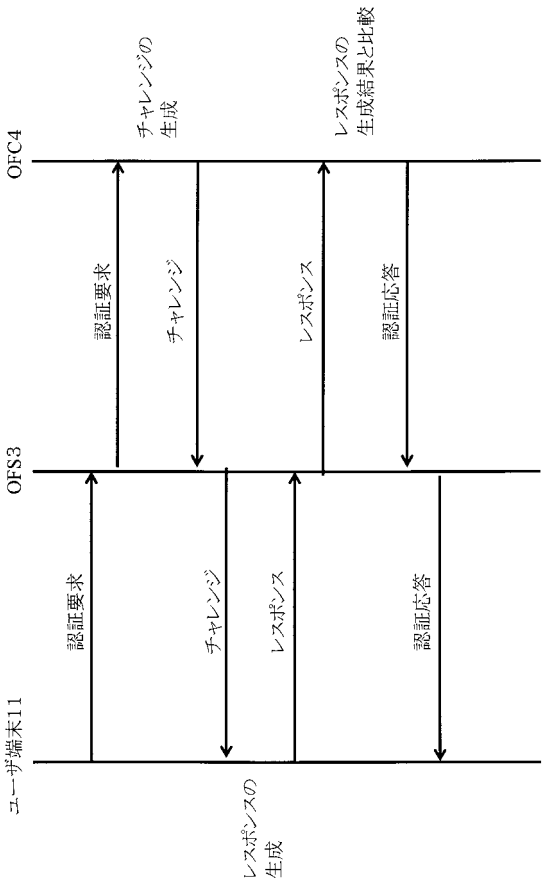
【図１０】



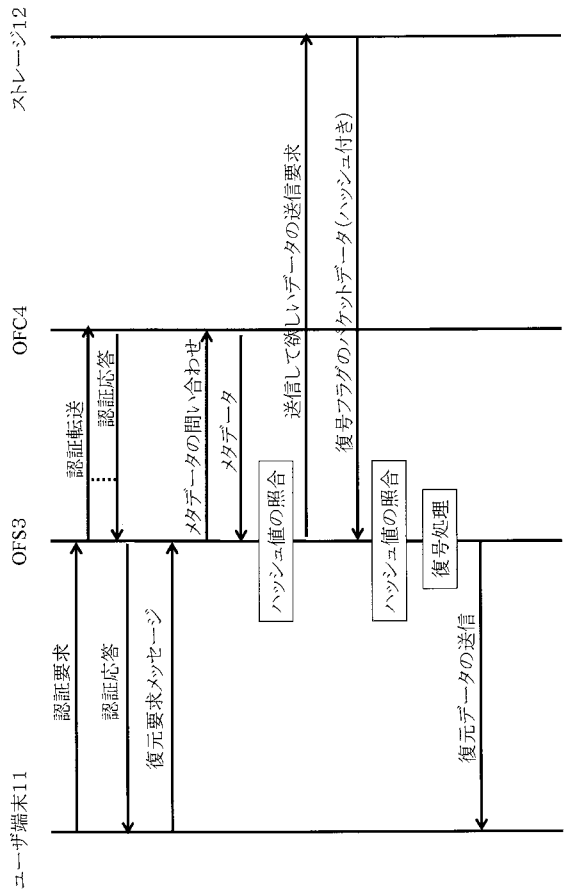
【図１１】



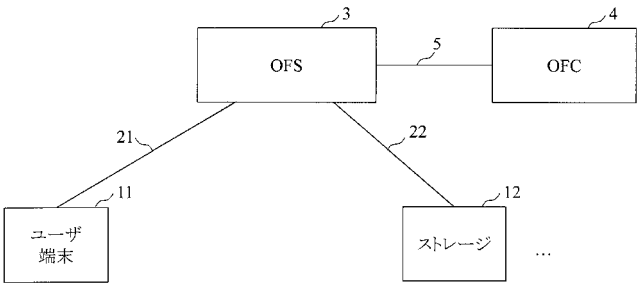
【図１２】



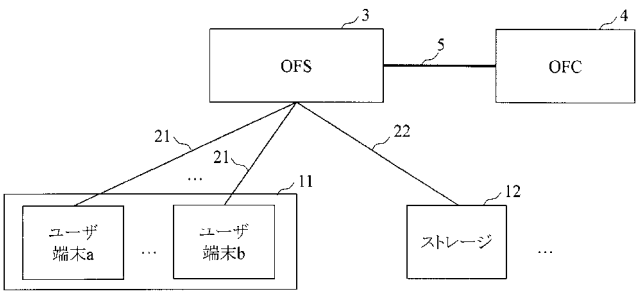
【図１３】



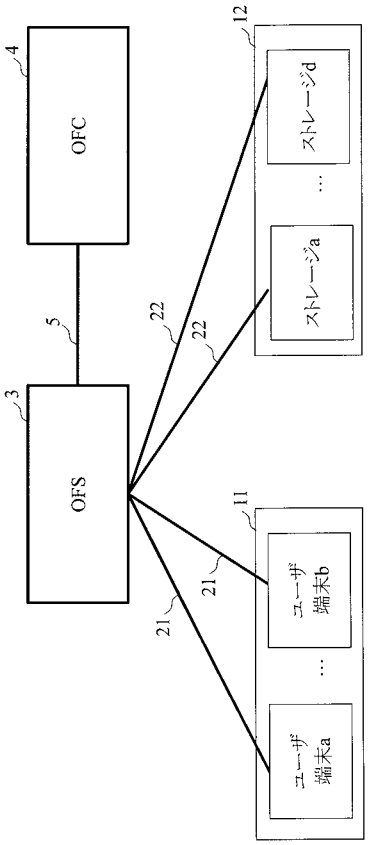
【図１４】



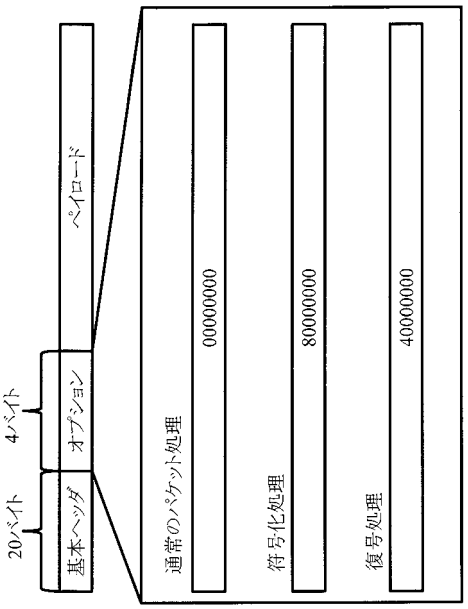
【図１５】



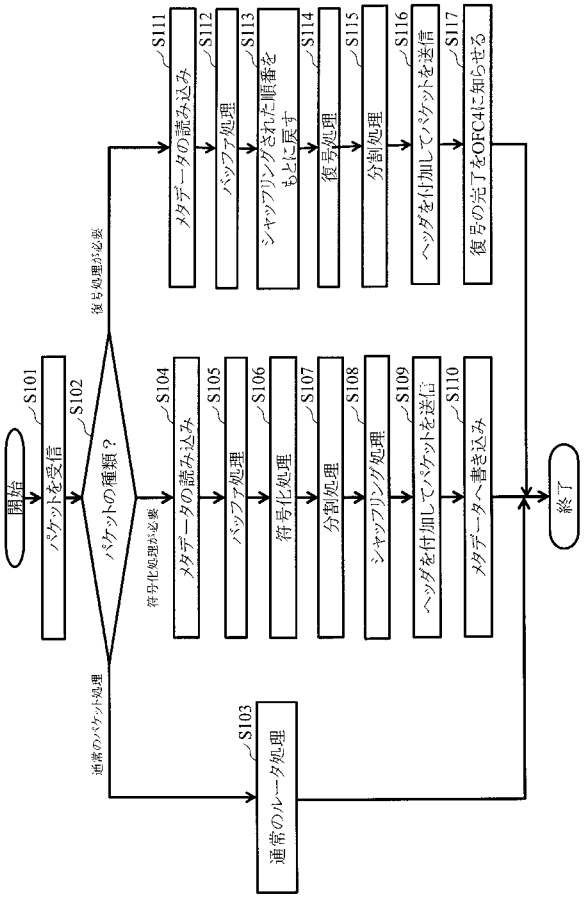
【図１６】



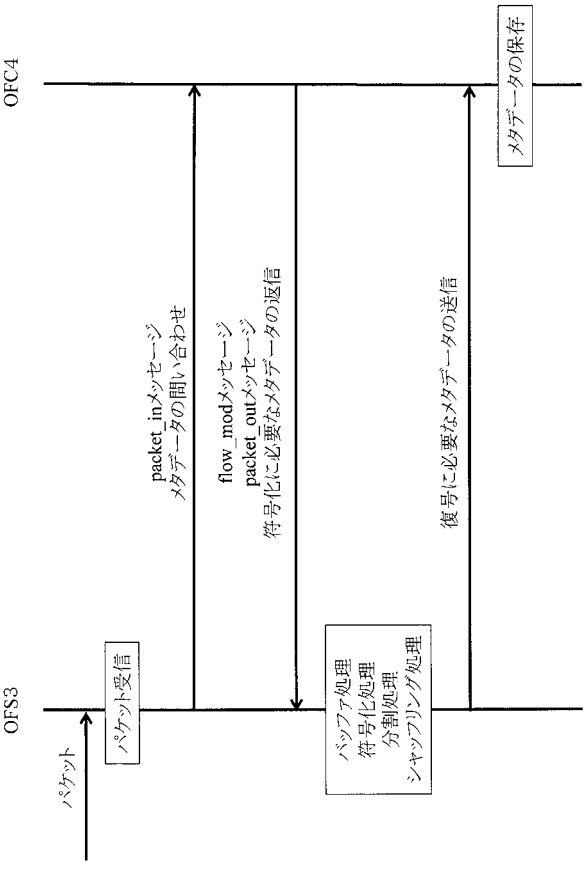
【図１７】



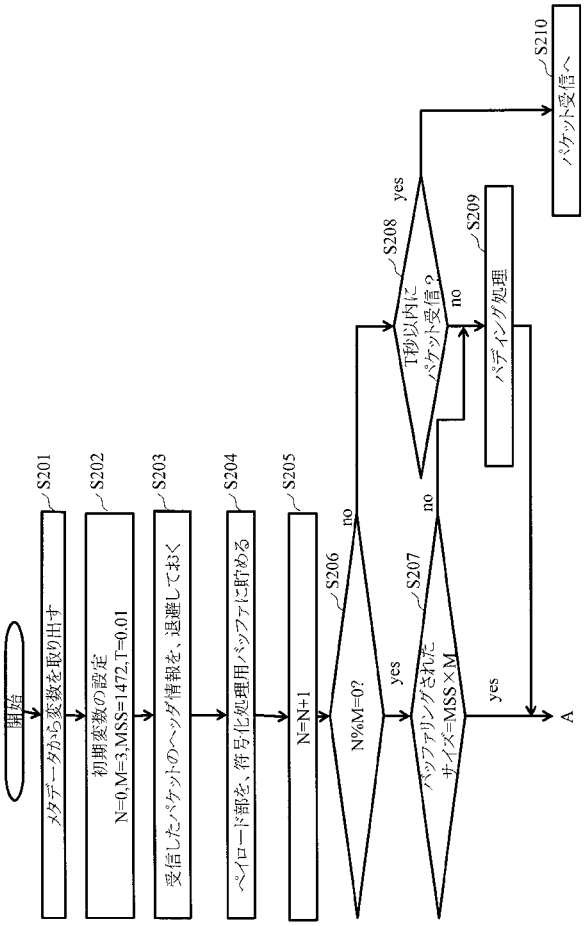
【図１８】



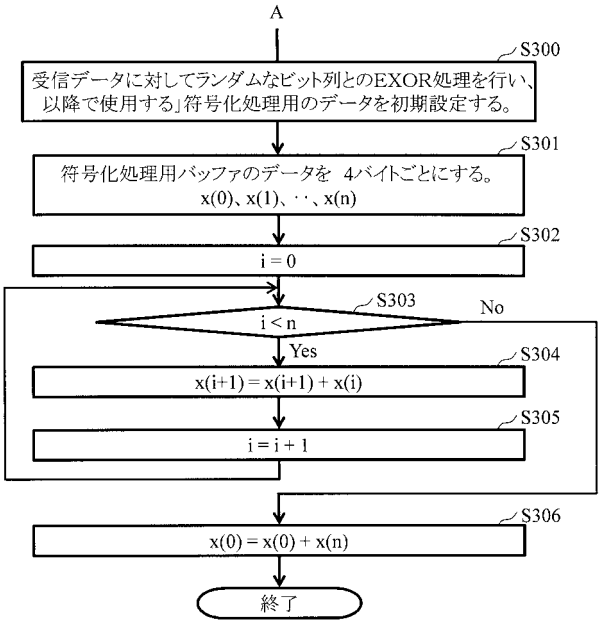
【図１９】



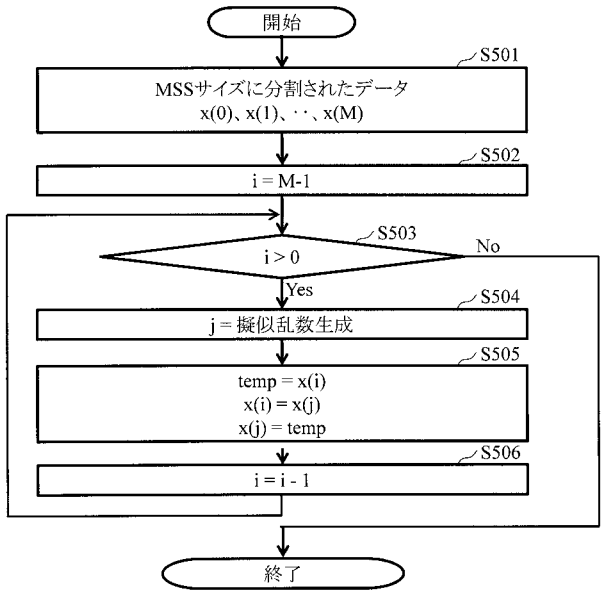
【図２０】



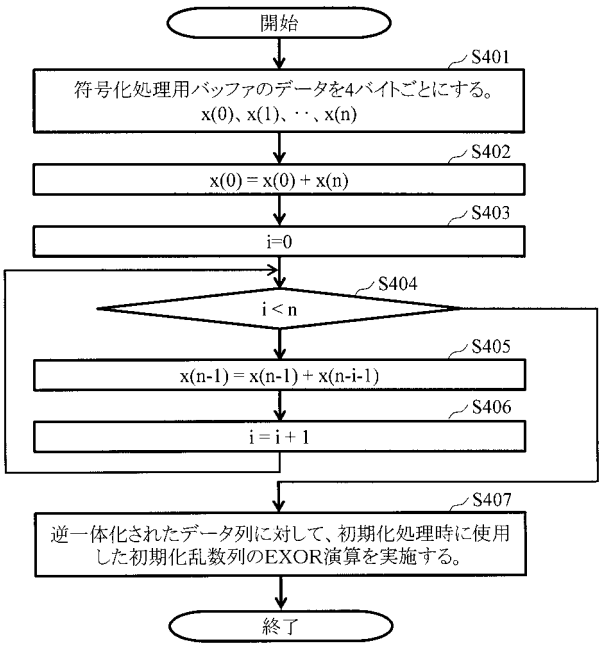
【図２１】



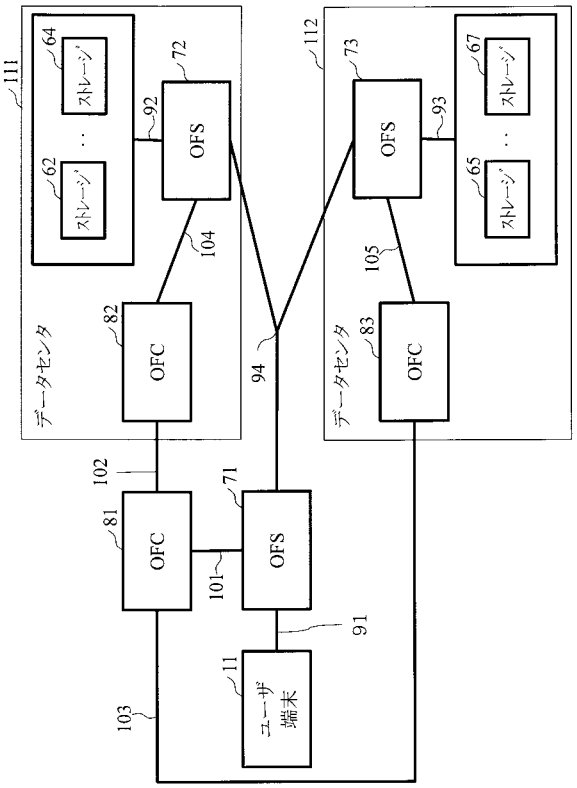
【図２２】



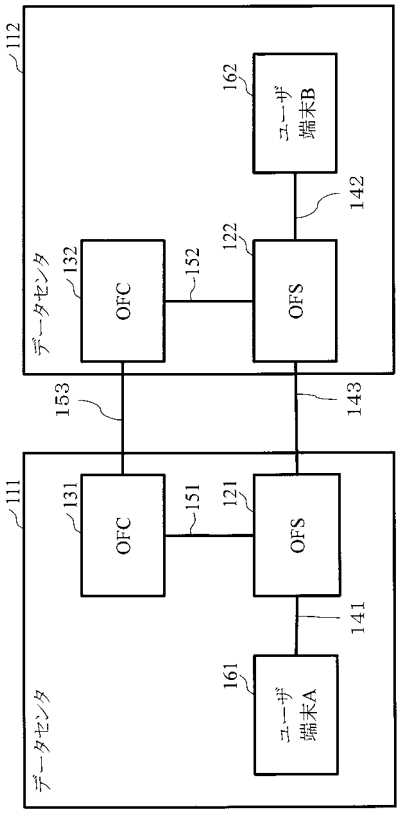
【図２３】



【図２４】


111
データセンタ
64
ストレージ
62
ストレージ
92
72
OFS
104
82
OFC
94
112
データセンタ
73
OFS
93
67
ストレージ
65
ストレージ
105
83
OFC
102
81
OFC
101
71
OFS
91
11
ユーザ端末
103

【図２５】


112
データセンタ
162
ユーザ端末B
142
132
OFC
152
122
OFS
153
143
111
データセンタ
131
OFC
151
121
OFS
141
161
ユーザ端末A

フロントページの続き

(72)発明者　鈴木　秀一
東京都足立区千住旭町５番　学校法人東京電機大学内
(72)発明者　古川　雅大
東京都足立区千住旭町５番　学校法人東京電機大学内

Ｆターム(参考) 5J104 AA07 AA16 AA32 BA02 EA08 EA17 KA02 NA06 NA09 NA12
NA38
5K030 GA15 HA08 HC01 HD03 LB07 LB11 LD19