(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7000090号
(P7000090)

(45)発行日　令和4年1月19日(2022.1.19)

(24)登録日　令和3年12月27日(2021.12.27)

(51)国際特許分類
Ｈ０４Ｌ　49/9057(2022.01)

ＦＩ
Ｈ０４Ｌ　49/9057

請求項の数　19　（全32頁）

(21)出願番号　特願2017-181740(P2017-181740)
(22)出願日　平成29年9月21日(2017.9.21)
(65)公開番号　特開2019-57846(P2019-57846A)
(43)公開日　平成31年4月11日(2019.4.11)
審査請求日　令和2年8月7日(2020.8.7)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(73)特許権者　598076591
東芝インフラシステムズ株式会社
神奈川県川崎市幸区堀川町７２番地３４
(74)代理人　100108855
弁理士　蔵田 昌俊
(74)代理人　100103034
弁理士　野河 信久
(74)代理人　100075672
弁理士　峰 隆司
(74)代理人　100153051
弁理士　河野 直樹
(74)代理人　100189913

最終頁に続く

(54)【発明の名称】　パケット集約装置、パケット分割装置、パケット通信システム、プログラム、パケット生成装置、パケット生成方法及び通信方法

(57)【特許請求の範囲】
【請求項１】
個別パケットを受信する受信部と、
前記受信部によって受信された複数の個別パケットを、暗号化済みでない部分が連続するように集約した集約パケットを生成し、生成した前記集約パケットのうちの暗号化済みでないと判定した範囲を暗号化する、処理部と、
前記処理部によって暗号化された前記集約パケットを送信する送信部と、を備えた、パケット集約装置。
【請求項２】
前記処理部は、生成した前記集約パケットのうちの、データの完全性を保証するための符号が付与されていないと判定した範囲に、データの完全性を保証するための符号を付与する、請求項１に記載のパケット集約装置。
【請求項３】
前記処理部は、
前記集約パケットを、前記集約パケットに含まれる個別パケット単位で暗号化し、　前記集約パケットに対して、前記集約パケットに含まれる個別パケット単位でデータの完全性を保証するための符号を付与する、請求項１又は請求項２に記載のパケット集約装置。
【請求項４】
前記処理部は、前記集約パケットを複数回送信させるように前記送信部を制御する、請求項１乃至請求項３のいずれか１項に記載のパケット集約装置。

【請求項５】
前記処理部は、前記集約パケットを少なくとも２種類の経路で送信させるように前記送信部を制御する、請求項４に記載のパケット集約装置。
【請求項６】
複数の個別パケットを、暗号化済みでない部分が連続するように集約した集約パケットを生成し、生成した前記集約パケットのうちの暗号化済みでないと判定した範囲を暗号化する、パケット集約装置によって生成され送信された前記集約パケットから、前記集約パケットに含まれる前記個別パケットを分割する、処理部を備えた、パケット分割装置。
【請求項７】
前記集約パケットに、データの完全性が保証されない個別パケットが含まれる場合、データの完全性が保証されない個別パケットを破棄する、請求項６に記載のパケット分割装置。
【請求項８】
前記集約パケットに含まれる集約ヘッダーのデータの完全性が保証されない場合、前記集約パケット全体を破棄する、請求項６又は請求項７に記載のパケット分割装置。
【請求項９】
前記集約パケットに含まれる個別パケットのうち、データの完全性が保証される個別パケットを到着済みとして記録し、
前記集約パケットに含まれる個別パケットのうち、到着済みとして記録されている個別パケットを破棄する、請求項６乃至請求項８のいずれか１項に記載のパケット分割装置。
【請求項１０】
前記集約パケットは、前記パケット集約装置によって、前記集約パケットに含まれる個別パケットのそれぞれに識別子を付与され、
前記処理部は、送信済みで且つ未到着の個別パケットを前記識別子によって判定し、未到着の個別パケットの再送を前記パケット集約装置に要求する、請求項６乃至請求項９のいずれか１項に記載のパケット分割装置。
【請求項１１】
パケット集約装置とパケット分割装置とを含み、
前記パケット集約装置は、
複数の個別パケットを、暗号化済みでない部分が連続するように集約した集約パケットを生成し、生成した前記集約パケットのうちの暗号化済みでないと判定した範囲を暗号化する、第１の処理部と、
複数の個別パケットが集約された集約パケットをパケット分割装置に送信する第１の通信部と、を備え、
前記パケット分割装置は、
前記パケット集約装置から送信された前記集約パケットを受信する第２の通信部と、
前記第２の通信部によって受信された集約パケットから、前記集約パケットに含まれる前記個別パケットを分割する第２の処理部と、を備える
パケット通信システム。
【請求項１２】
パケット集約装置が備えるコンピュータを、
複数の個別パケットを、暗号化済みでない部分が連続するように集約して、複数の個別パケットを含む集約パケットを生成し、生成した前記集約パケットのうちの暗号化済みでないと判定した範囲を暗号化し、処理部として機能させる、プログラム。
【請求項１３】
パケット分割装置が備えるコンピュータを、
複数の個別パケットを、暗号化済みでない部分が連続するように集約した集約パケットを生成し、生成した前記集約パケットのうちの暗号化済みでないと判定した範囲を暗号化する、パケット集約装置によって生成され送信された前記集約パケットから、前記集約パケットに含まれる前記個別パケットを分割する、処理部として機能させる、プログラム。
【請求項１４】

パケットを受信する受信部と、前記受信部によって受信された複数のパケットを、暗号化済みでない部分が連続するように集約した集約パケットデータを生成し、生成した前記集約パケットデータのうちの暗号化済みでないと判定した範囲を暗号化する、生成部を備え、
前記集約パケットデータは、前記複数のパケットのそれぞれがヘッダー部とペイロード部とを含み、前記集約パケットデータに含まれる複数のペイロード部が複数の鍵で暗号化され、前記集約パケットデータに含まれる複数のヘッダー部が同一の鍵で暗号化されている、パケット生成装置。
【請求項１５】
前記集約パケットデータは、複数の前記ヘッダー部が連続している、請求項１４に記載のパケット生成装置。
【請求項１６】
前記集約パケットデータは、前記パケットのそれぞれに対してデータの完全性を保証するための符号と識別子とが付与されている、請求項１４に記載のパケット生成装置。
【請求項１７】
パケットを受信し、受信された複数のパケットを、暗号化済みでない部分が連続するように集約した集約パケットデータを生成し、生成した前記集約パケットデータのうちの暗号化済みでないと判定した範囲を暗号化する、パケット生成方法であって、
前記集約パケットデータは、前記複数のパケットのそれぞれがヘッダー部とペイロード部とを含み、前記集約パケットデータに含まれる複数のペイロード部が複数の鍵で暗号化され、前記集約パケットデータに含まれる複数のヘッダー部が同一の鍵で暗号化されている、パケット生成方法。
【請求項１８】
パケット生成装置が備えるコンピュータを、
パケットを受信する受信部と、前記受信部によって受信された複数のパケットを、暗号化済みでない部分が連続するように集約した集約パケットデータを生成し、生成した前記集約パケットデータのうちの暗号化済みでないと判定した範囲を暗号化する、生成部として機能させ、
前記集約パケットデータは、前記複数のパケットのそれぞれがヘッダー部とペイロード部とを含み、前記集約パケットデータに含まれる複数のペイロード部が複数の鍵で暗号化され、前記集約パケットデータに含まれる複数のヘッダー部が同一の鍵で暗号化されている、プログラム。
【請求項１９】
複数の個別パケットが、暗号化済みでない部分が連続するように集約された集約パケットが生成され、前記集約パケットのうちの暗号化済みでないと判定された範囲が暗号化され、前記個別パケットが個別パケット単位でデータの完全性を保証するための符号を付与された前記集約パケットを受信し、
受信した前記集約パケットに、データの完全性が保証されない前記個別パケットが含まれる場合、データの完全性が保証されない前記個別パケットの再送を要求する、通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、パケット集約装置、パケット分割装置、パケット通信システム、プログラム、パケット生成装置、パケット生成方法及び通信方法に関する。
【背景技術】
【０００２】
クライアントサーバーモデルのシステムなどにおいて、クライアントからサーバーに対して多数のアクサスが発生する場合がある。このような場合、ネットワーク又はサーバーなどに対する負荷が増大する。特に、小さいサイズのパケットを大量に処理する場合には、サーバーのネットワークインターフェースなどに対する処理負荷が増大する。
【先行技術文献】

【特許文献】
【０００３】
【文献】特開２００３－１６９０９２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
本発明の実施形態が解決しようとする課題は、処理負荷を低減し、リアルタイム性の低下を抑える、パケット集約装置、パケット分割装置、パケット通信システム、プログラム、パケット生成装置、パケット生成方法及び通信方法を提供することである。
【課題を解決するための手段】
【０００５】
実施形態のパケット処理装置は、受信部、処理部及び送信部を含む。受信部は、個別パケットを受信する。処理部は、前記受信部によって受信された複数の個別パケットを集約した集約パケットを生成し、生成した前記集約パケットのうちの暗号化済みでないと判定した範囲を暗号化する。送信部は、前記処理部によって暗号化された集約パケットを送信する。
【図面の簡単な説明】
【０００６】
【図１】第１実施形態及び第２実施形態に係る通信システム及び当該通信システムに含まれる装置の要部回路構成を示すブロック図。
【図２】図１中のパケット集約装置の第１実施形態に係る機能構成を示すブロック図。
【図３】図１中のパケット集約装置が備えるプロセッサーによる第１実施形態～第３実施形態に係る処理の一例を示すフローチャート。
【図４】図１中のパケット集約装置が備えるプロセッサーによる第１実施形態及び第２実施形態に係る処理の一例を示すフローチャート。
【図５】図１中のパケット集約装置が備えるプロセッサーによる第１実施形態及び第２実施形態に係る処理の一例を示すフローチャート。
【図６】図１中のサーバー装置が備えるプロセッサーによる第１実施形態及び第２実施形態に係る処理の一例を示すフローチャート。
【図７】図１中のサーバー装置が備えるプロセッサーによる第１実施形態及び第２実施形態に係る処理の一例を示すフローチャート。
【図８】図１中のサーバー装置が備えるプロセッサーによる第１実施形態～第３実施形態に係る処理の一例を示すフローチャート。
【図９】第１実施形態に係る集約パケットの一例を説明するための図。
【図１０】第２実施形態に係る集約パケットの一例を説明するための図。
【図１１】図１中のパケット集約装置の第３実施形態に係る機能構成を示すブロック図。
【図１２】図１中のパケット集約装置が備えるプロセッサーによる第３実施形態に係る処理の一例を示すフローチャート。
【図１３】図１中のパケット集約装置が備えるプロセッサーによる第３実施形態に係る処理の一例を示すフローチャート。
【図１４】第３実施形態に係る集約パケットの一例を説明するための図。
【図１５】第３実施形態に係る通信システムの情報の流れの一例を示すシーケンス図。
【発明を実施するための形態】
【０００７】
以下、いくつかの実施形態に係る通信システムについて図面を用いて説明する。
〔第１実施形態〕
図１は、第１実施形態に係る通信システム１及び通信システム１に含まれる構成要素の要部回路構成の一例を示すブロック図である。通信システム１は、パケット処理装置１０、サーバー装置２０及びクライアント装置３０を含む。通信システム１は、一例として、サーバー装置２０とクライアント装置３０との間で通信を行う、サーバークライアントモデ

ルのシステムである。なお、図１にはパケット処理装置１０を１台、サーバー装置２０を１台、クライアント装置３０を３台示しているが、これらの台数に限定するものではない。
【０００８】
パケット処理装置１０及びクライアント装置３０は、ネットワークＮＷ１に接続されている。ネットワークＮＷ１は、典型的にはＬＡＮ（local area network）を含む通信網である。ネットワークＮＷ１は、典型的にはイントラネットなどのプライベートネットワークを含む通信網である。ネットワークＮＷ１は、インターネットを含む通信網であっても良い。ネットワークＮＷ１は、ＷＡＮ（wide area network）を含む通信網であっても良い。
パケット処理装置１０及びサーバー装置２０は、ネットワークＮＷ２に接続されている。ネットワークＮＷ２は、典型的には、インターネットを含む通信網である。ネットワークＮＷは１、典型的には、ＷＡＮを含む通信網である。ネットワークＮＷ２は、イントラネットなどのプライベートネットワークを含む通信網であっても良い。ネットワークＮＷ２は、ＬＡＮを含む通信網であっても良い。
ネットワークＮＷ１及びネットワークＮＷ２のそれぞれは、携帯電話回線網、専用線、又はその他の通信網を含む通信網であっても良い。
ネットワークＮＷ１及びネットワークＮＷ２上の通信は、パケット通信によって行われる。
【０００９】
パケット処理装置１０は、例えばゲートウェイ又はルーターなどである。パケット処理装置１０は、サーバー装置２０とクライアント装置３０との間の通信を中継する。パケット処理装置１０は、クライアント装置３０などから送信された複数のパケットを１つのパケットに集約する機能を有する。なお、複数のパケットが集約されたパケットを、以下「集約パケット」という。また、集約パケットでないパケットを、以下「個別パケット」という。また、パケット処理装置１０は、サーバー装置２０などから送信された集約パケットを個々の個別パケットに分割する機能を有する。さらに、パケット処理装置１０は、集約パケットを暗号化する機能、及び暗号化された集約パケットを復号する機能を有する。パケット処理装置１０は、プロセッサー１１、ＲＯＭ（read-only memory）１２、ＲＡＭ（random-access memory）１３、補助記憶デバイス１４、第１の通信Ｉ／Ｆ（interface）１５及び第２の通信Ｉ／Ｆ１６を含む。パケット処理装置１０は、パケット集約装置の一例である。パケット処理装置１０は、パケット分割装置の一例である。パケット処理装置１０は、パケット生成装置の一例である。
【００１０】
プロセッサー１１は、パケット処理装置１０の動作に必要な演算及び制御などの処理を行うコンピューターの中枢部分に相当する。プロセッサー１１は、ＲＯＭ１２又は補助記憶デバイス１４などに記憶されたシステムソフトウェア、アプリケーションソフトウェア又はファームウェアなどのプログラムに基づいて、パケット処理装置１０の各種の機能を実現するべく各部を制御する。プロセッサー１１は、例えば、ＣＰＵ（central processing unit）、ＭＰＵ（micro processing unit）、ＳｏＣ（system on a chip）、ＤＳＰ（digital signal processor）、ＧＰＵ（graphics processing unit）、ＡＳＩＣ（application specific integrated circuit）、ＰＬＤ（programmable logic device）又はＦＰＧＡ（field-programmable gate array）などである。あるいは、プロセッサー１１は、これらの組み合わせである。プロセッサー１１は、処理部の一例である。プロセッサー１１は、第１の処理部の一例である。プロセッサー１１は、第２の処理部の一例である。プロセッサー１１は、生成部の一例である。プロセッサー１１を中枢とするコンピューターは、処理部の値例である。プロセッサー１１を中枢とするコンピューターは、第１の処理部の一例である。プロセッサー１１を中枢とするコンピューターは、第２の処理部の一例である。プロセッサー１１を中枢とするコンピューターは、生成部の一例である。
【００１１】
ＲＯＭ１２は、プロセッサー１１を中枢とするコンピューターの主記憶装置に相当する。ＲＯＭ１２は、専らデータの読み出しに用いられる不揮発性メモリである。ＲＯＭ１２は

、上記のプログラムを記憶する。また、ＲＯＭ１２は、プロセッサー１１が各種の処理を行う上で使用するデータ又は各種の設定値などを記憶する。

【００１２】

ＲＡＭ１３は、プロセッサー１１を中枢とするコンピューターの主記憶装置に相当する。ＲＡＭ１３は、データの読み書きに用いられるメモリである。ＲＡＭ１３は、プロセッサー１１が各種の処理を行う上で一時的に使用するデータを記憶しておく、いわゆるワークエリアなどとして利用される。

【００１３】

補助記憶デバイス１４は、プロセッサー１１を中枢とするコンピューターの補助記憶装置に相当する。補助記憶デバイス１４は、例えばＥＥＰＲＯＭ（electric erasable programmable read-only memory）、ＨＤＤ（hard disk drive）又はＳＳＤ（solid state drive）などである。補助記憶デバイス１４は、上記のプログラムを記憶する場合がある。また、補助記憶デバイス１４は、プロセッサー１１が各種の処理を行う上で使用するデータ、プロセッサー１１での処理によって生成されたデータ又は各種の設定値などを保存する。

【００１４】

ＲＯＭ１２又は補助記憶デバイス１４に記憶されるプログラムは、後述する処理を実行するためのプログラムを含む。一例として、パケット処理装置１０は、当該プログラムがＲＯＭ１２又は補助記憶デバイス１４に記憶された状態でパケット処理装置１０の管理者などへと譲渡される。しかしながら、パケット処理装置１０は、当該プログラムがＲＯＭ１２又は補助記憶デバイス１４に記憶されない状態で当該管理者などに譲渡されても良い。また、パケット処理装置１０は、当該プログラムとは別のプログラムがＲＯＭ１２又は補助記憶デバイス１４に記憶された状態で当該管理者などに譲渡されても良い。そして、後述する処理を実行するためのプログラムが別途に当該管理者などへと譲渡され、当該管理者又はサービスマンなどによる操作の下にＲＯＭ１２又は補助記憶デバイス１４へと書き込まれても良い。このときのプログラムの譲渡は、例えば、磁気ディスク、光磁気ディスク、光ディスク又は半導体メモリなどのようなリムーバブルな記憶媒体に記録して、あるいはネットワークを介したダウンロードにより実現できる。

【００１５】

第１の通信Ｉ／Ｆ１５は、パケット処理装置１０がネットワークＮＷ１などを介して通信するためのインターフェースである。第１の通信Ｉ／Ｆ１５は、個別パケットを受信する受信部の一例である。第１の通信Ｉ／Ｆ１５は、個別パケットを受信する第４の通信部の一例である。

【００１６】

第２の通信Ｉ／Ｆ１６は、パケット処理装置１０がネットワークＮＷ２などを介して通信するためのインターフェースである。第２の通信Ｉ／Ｆ１６は、集約パケットを送信する送信部の一例である。第２の通信Ｉ／Ｆ１６は、集約パケットをパケット分割装置に送信する第１の通信部の一例である。第２の通信Ｉ／Ｆ１６は、集約パケットを受信する第２の通信部の一例である。

【００１７】

サーバー装置２０は、複数のクライアント装置３０と通信を行う。サーバー装置２０は、例えば、クライアント装置３０から送信された要求に応じて各種処理などを行う。サーバー装置２０は、プロセッサー２１、ＲＯＭ２２、ＲＡＭ２３、補助記憶デバイス２４及び通信Ｉ／Ｆ２５を含む。サーバー装置２０は、パケット集約装置の一例である。サーバー装置２０は、パケット分割装置の一例である。サーバー装置２０は、パケット生成装置の一例である。

【００１８】

プロセッサー２１は、サーバー装置２０の動作に必要な演算及び制御などの処理を行うコンピューターの中枢部分に相当する。プロセッサー２１は、ＲＯＭ２２又は補助記憶デバイス２４などに記憶されたシステムソフトウェア、アプリケーションソフトウェア又はフ

ァームウェアなどのプログラムに基づいて、サーバー装置２０の各種の機能を実現するべく各部を制御する。プロセッサー２１は、例えば、ＣＰＵ、ＭＰＵ、ＳｏＣ、ＤＳＰ、ＧＰＵ、ＡＳＩＣ、ＰＬＤ又はＦＰＧＡなどである。あるいは、プロセッサー２１は、これらの組み合わせである。プロセッサー２１は、処理部の一例である。プロセッサー２１は、第１の処理部の一例である。プロセッサー２１は、第２の処理部の一例である。プロセッサー２１は、生成部の一例である。プロセッサー２１を中枢とするコンピューターは、処理部の値例である。プロセッサー２１を中枢とするコンピューターは、第１の処理部の一例である。プロセッサー２１を中枢とするコンピューターは、第２の処理部の一例である。プロセッサー２１を中枢とするコンピューターは、生成部の一例である。

【００１９】

ＲＯＭ２２は、プロセッサー２１を中枢とするコンピューターの主記憶装置に相当する。ＲＯＭ２２は、専らデータの読み出しに用いられる不揮発性メモリである。ＲＯＭ２２は、上記のプログラムを記憶する。また、ＲＯＭ２２は、プロセッサー２１が各種の処理を行う上で使用するデータ又は各種の設定値などを記憶する。

【００２０】

ＲＡＭ２３は、プロセッサー２１を中枢とするコンピューターの主記憶装置に相当する。ＲＡＭ２３は、データの読み書きに用いられるメモリである。ＲＡＭ２３は、プロセッサー２１が各種の処理を行う上で一時的に使用するデータを記憶しておく、いわゆるワークエリアなどとして利用される。

【００２１】

補助記憶デバイス２４は、プロセッサー２１を中枢とするコンピューターの補助記憶装置に相当する。補助記憶デバイス２４は、例えばＥＥＰＲＯＭ、ＨＤＤ又はＳＳＤなどである。補助記憶デバイス２４は、上記のプログラムを記憶する場合がある。また、補助記憶デバイス２４は、プロセッサー２１が各種の処理を行う上で使用するデータ、プロセッサー２１での処理によって生成されたデータ又は各種の設定値などを保存する。

【００２２】

ＲＡＭ２３又は補助記憶デバイス２４は、処理バッファー及びサーバー集約バッファーを含む。処理バッファーは、未処理のパケットを記憶する。サーバー集約バッファーは、未集約未送信のパケットを記憶する。

【００２３】

ＲＯＭ２２又は補助記憶デバイス２４に記憶されるプログラムは、後述する処理を実行するためのプログラムを含む。一例として、サーバー装置２０は、当該プログラムがＲＯＭ２２又は補助記憶デバイス２４に記憶された状態でサーバー装置２０の管理者などへと譲渡される。しかしながら、サーバー装置２０は、当該プログラムがＲＯＭ２２又は補助記憶デバイス２４に記憶されない状態で当該管理者などに譲渡されても良い。また、サーバー装置２０は、当該プログラムとは別のプログラムがＲＯＭ２２又は補助記憶デバイス２４に記憶された状態で当該管理者などに譲渡されても良い。そして、後述する処理を実行するためのプログラムが別途に当該管理者などへと譲渡され、当該管理者又はサービスマンなどによる操作の下にＲＯＭ２２又は補助記憶デバイス２４へと書き込まれても良い。このときのプログラムの譲渡は、例えば、磁気ディスク、光磁気ディスク、光ディスク又は半導体メモリなどのようなリムーバブルな記憶媒体に記録して、あるいはネットワークを介したダウンロードにより実現できる。

【００２４】

通信Ｉ／Ｆ２５は、サーバー装置２０がネットワークＮＷ２などを介して通信するためのインターフェースである。通信Ｉ／Ｆ２５は、集約パケットをパケット分割装置に送信する第１の通信部の一例である。通信Ｉ／Ｆ２５は、集約パケットを受信する第２の通信部の一例である。

【００２５】

クライアント装置３０は、例えば、自動券売機、自動精算機若しくは自動改札機などの駅務装置、ＰＣ（personal computer）、サーバー若しくはスマートホンなどの情報機器

、又は各種ＩｏＴ（internet of things）機器などである。クライアント装置３０は、プロセッサー３１、ＲＯＭ３２、ＲＡＭ３３、補助記憶デバイス３４及び通信Ｉ／Ｆ３５を含む。

【００２６】

プロセッサー３１は、クライアント装置３０の動作に必要な演算及び制御などの処理を行うコンピューターの中枢部分に相当する。プロセッサー３１は、ＲＯＭ３２又は補助記憶デバイス３４などに記憶されたシステムソフトウェア、アプリケーションソフトウェア又はファームウェアなどのプログラムに基づいて、クライアント装置３０の各種の機能を実現するべく各部を制御する。プロセッサー３１は、例えば、ＣＰＵ、ＭＰＵ、ＳｏＣ、ＤＳＰ、ＧＰＵ、ＡＳＩＣ、ＰＬＤ又はＦＰＧＡなどである。あるいは、プロセッサー３１は、これらの組み合わせである。

【００２７】

ＲＯＭ３２は、プロセッサー３１を中枢とするコンピューターの主記憶装置に相当する。ＲＯＭ３２は、専らデータの読み出しに用いられる不揮発性メモリである。ＲＯＭ３２は、上記のプログラムを記憶する。また、ＲＯＭ３２は、プロセッサー３１が各種の処理を行う上で使用するデータ又は各種の設定値などを記憶する。

【００２８】

ＲＡＭ３３は、プロセッサー３１を中枢とするコンピューターの主記憶装置に相当する。ＲＡＭ３３は、データの読み書きに用いられるメモリである。ＲＡＭ３３は、プロセッサー３１が各種の処理を行う上で一時的に使用するデータを記憶しておく、いわゆるワークエリアなどとして利用される。

【００２９】

補助記憶デバイス３４は、プロセッサー３１を中枢とするコンピューターの補助記憶装置に相当する。補助記憶デバイス３４は、例えばＥＥＰＲＯＭ、ＨＤＤ又はＳＳＤなどである。補助記憶デバイス３４は、上記のプログラムを記憶する場合がある。また、補助記憶デバイス３４は、プロセッサー３１が各種の処理を行う上で使用するデータ、プロセッサー３１での処理によって生成されたデータ又は各種の設定値などを保存する。

【００３０】

通信Ｉ／Ｆ３５は、クライアント装置３０がネットワークＮＷ１などを介して通信するためのインターフェースである。通信Ｉ／Ｆ３５は、個別パケットを前記パケット集約装置に送信する第３の通信部の一例である。

【００３１】

パケット処理装置１０について、図２を用いてさらに説明する。図２は、パケット処理装置１０の機能構成を示すブロック図である。なお、図２おける図１と同様の要素については同一の符号を付している。パケット処理装置１０は、第１受信部１０１、集約バッファー１０２、周期管理部１０３、結合部１０４、範囲選択部１０５、暗号化部１０６、第１送信部１０７、第２受信部１０８、復号部１０９、分割部１１０及び第２送信部１１１を含む。

【００３２】

第１受信部１０１は、クライアント装置３０などから送信された個別パケットを受信する。例えば、第１の通信Ｉ／Ｆ１５が、第１受信部１０１として機能する。

【００３３】

集約バッファー１０２は、第１受信部１０１によって受信された個別パケットを記憶する。例えば、ＲＡＭ１３又は補助記憶デバイス１４が集約バッファー１０２として機能する。

【００３４】

周期管理部１０３は、一定周期ごとに集約バッファー１０２から個別パケットを取り出す。例えば、プロセッサー１１が周期管理部１０３として機能する。

【００３５】

結合部１０４は、周期管理部１０３によって取り出された複数の個別パケットを結合して集約する。結合部１０４は、集約パケットを生成する。例えば、プロセッサー１１が結合

部１０４として機能する。
【００３６】
範囲選択部１０５は、集約パケットのうちの暗号化する範囲を決定して選択する。例えば、プロセッサー１１が範囲選択部１０５として機能する。
【００３７】
暗号化部１０６は、集約パケットを暗号化する。また、暗号化部１０６は、集約パケットの暗号化と共に、当該集約パケットのＭＡＣ（message authentication code）値を生成する。ＭＡＣ値は、集約パケットの改竄検出など、集約パケットのデータの完全性の検証に用いられる。例えば、プロセッサー１１が暗号化部１０６として機能する。ＭＡＣ値は、データの完全性を保証するための符号の一例である。
【００３８】
第１送信部１０７は、周期管理部１０３、範囲選択部１０５、結合部１０４及び暗号化部１０６によって生成された集約パケットをサーバー装置２０などに送信する。例えば、第２の通信Ｉ／Ｆ１６が、第１送信部１０７として機能する。
【００３９】
第２受信部１０８は、サーバー装置２０などから集約パケットを受信する。例えば、第２の通信Ｉ／Ｆ１６が、第２受信部１０８として機能する。
【００４０】
復号部１０９は、第２受信部によって受信された集約パケットの暗号化された部分を復号する。また、復号部１０９は、当該集約パケットに含まれるＭＡＣ値を用いてデータの完全性の検証を行う。さらに、復号部１０９は、集約パケットが改竄されたことなどによりデータの完全性の保証が得られなかった場合には、当該集約パケットを破棄する。例えば、プロセッサー１１が復号部１０９として機能する。
【００４１】
分割部１１０は、第２受信部によって受信された集約パケットを個々の個別パケットに分割する。例えば、プロセッサー１１が分割部１１０として機能する。
【００４２】
第２送信部１１１は、分割部１１０によって分割された個々の個別パケットのそれぞれを、それぞれの個別パケットの宛先であるクライアント装置３０などに送信する。例えば、第１の通信Ｉ／Ｆ１５が、第２送信部１１１として機能する。
【００４３】
以下、第１実施形態に係る通信システム１の動作を図３～図８に基づいて説明する。なお、以下の動作説明における処理の内容は一例であって、同様な結果を得ることが可能な様々な処理を適宜に利用できる。図３～図５は、パケット処理装置１０のプロセッサー１１による処理のフローチャートである。プロセッサー１１は、ＲＯＭ１２又は補助記憶デバイス１４などに記憶されたプログラムに基づいてこの処理を実行する。なお、プロセッサー１１は、図３～図５に示す処理を並行又は並列して処理する。図６～８は、サーバー装置２０のプロセッサー２１による処理のフローチャートである。プロセッサー２１は、ＲＯＭ２２又は補助記憶デバイス２４などに記憶されたプログラムに基づいてこの処理を実行する。なお、プロセッサー２１は、図６～図８に示す処理を並行又は並列して処理する。また、特に説明が無い限り、プロセッサー１１及びプロセッサー２１は、ステップＳ（ｍ）（ｍは、自然数。）の処理の後、ステップＳ（ｍ＋１）へと進むものとする。
【００４４】
複数のクライアント装置３０のそれぞれは、サーバー装置２０を宛先とするデータを送信する。当該データは、個別パケットとして送信される。当該個別パケットは、ネットワークＮＷ１を介してパケット処理装置１０によって受信される。
図３のステップＳ１においてプロセッサー１１は、第１の通信Ｉ／Ｆ１５（第１受信部１０１）によって、クライアント装置３０から送信された個別パケットが受信されるのを待ち受けている。プロセッサー１１は、個別パケットが受信されたならば、ステップＳ１においてＹｅｓと判定してステップＳ２へと進む。

【００４５】
ステップＳ２においてプロセッサー１１は、ステップＳ１で受信された個別パケットを集約バッファー１０２に記憶させる。プロセッサー１１は、ステップＳ２の後、ステップＳ１へと戻る。
以上のようにして、第１の通信Ｉ／Ｆ１５によって受信された個別パケットが次々と集約バッファー１０２に蓄積記憶されていく。
【００４６】
一方、図４のステップＳ１１においてパケット処理装置１０のプロセッサー１１（周期管理部１０３）は、第１のタイマーをリセットする。第１のタイマーは、パケット処理装置１０が前回集約パケットを送信してからの経過時間を計測するためのタイマーである。なお、集約パケットについては、後述する。
【００４７】
ステップＳ１２においてプロセッサー１１（周期管理部１０３）は、第１のタイマーをリセットしてから時間Ｔ１以上経過したか否かを判定する。なお、時間Ｔ１は、例えば、パケット処理装置１０の管理者などによって予め設定される。あるいは、時間Ｔ１は、パケット処理装置１０の設計者などによって予め定められていてもよい。プロセッサー１１は、第１のタイマーをリセットしてから時間Ｔ１が経過していないならば、ステップＳ１２においてＮｏと判定してステップＳ１３へと進む。
【００４８】
ステップＳ１３においてプロセッサー１１は、集約バッファー１０２に記憶された未送信の個別パケットのデータ容量の合計が容量Ｄ１以上であるか否かを判定する。なお、容量Ｄ１は、例えば、パケット処理装置１０の管理者などによって予め設定される。あるいは、容量Ｄ１は、パケット処理装置１０の設計者などによって予め定められていてもよい。容量Ｄ１は、例えば、パケット処理装置１０が生成する集約パケットのＭＴＵ（maximum transmission unit）である。プロセッサー１１は、集約バッファー１０２に記憶された未送信の個別パケットのデータ容量の合計が容量Ｄ１以上でないならば、ステップＳ１３においてＮｏと判定してステップＳ１２へと戻る。かくして、プロセッサー１１は、第１のタイマーをリセットしてから時間Ｔ１が経過したか、集約バッファー１０２に記憶された未送信の個別パケットのデータ容量の合計が容量Ｄ１以上となるまでステップＳ１２及びステップＳ１３を繰り返す。すなわち、ステップＳ１２の処理により、一定周期ごとにステップＳ１４～ステップＳ２２の処理が繰り返される。
【００４９】
プロセッサー１１は、ステップＳ１２及びステップＳ１３の待受状態にあるときに、第１のタイマーをリセットしてから時間Ｔ１が経過したならば、ステップＳ１２においてＹｅｓと判定してステップＳ１４へと進む。
【００５０】
ステップＳ１４においてプロセッサー１１（周期管理部１０３）は、集約バッファー１０２に未送信の個別パケットが記憶されているか否かを判定する。プロセッサー１１は、集約バッファー１０２に未送信の個別パケットが記憶されていないならば、ステップＳ１４においてＮｏと判定してステップＳ１１へと戻る。すなわち、プロセッサー１１は、前回集約パケットを送信してから時間Ｔ１が経過しても未送信の個別パケットが集約バッファー１０２に記憶されなかったならば、第１のタイマーをリセットする。対して、プロセッサー１１は、集約バッファー１０２に未送信の個別パケットが記憶されているならば、ステップＳ１４においてＹｅｓと判定してステップＳ１５へと進む。
また、プロセッサー１１は、ステップＳ１２及びステップＳ１３の待受状態にあるときに集約バッファー１０２に記憶された未送信の個別パケットのデータ容量の合計が容量Ｄ１以上であるならば、ステップＳ１３においてＹｅｓと判定してステップＳ１５へと進む。
【００５１】
ステップＳ１５においてプロセッサー１１（周期管理部１０３）は、集約バッファー１０２に記憶された未送信の個別パケット１個を取り出す。ここで、プロセッサー１１は、個

別パケットを取り出すとき、集約バッファー１０２に記憶された当該個別パケットが送信済みであることが分かるようにする。あるいは、プロセッサー１１は、当該個別パケットを集約バッファーから削除する。当該個別パケットは、例えば、集約バッファー１０２に記憶されている未送信の個別パケットの中で最初に記憶された個別パケットである。そして、ステップＳ１５においてプロセッサー１１（結合部１０４）は、取り出したパケットを含む集約パケットを生成する。ここで生成される集約パケットの一例について、図９を用いて説明する。図９は、第１実施形態に係る集約パケットの一例を説明するための図である。なお、図９には、ｎ個の個別パケットが集約された集約パケットが示されているが、ステップＳ１５で生成される集約パケットに含まれる個別パケットは１つである。すなわち、ｎ＝１である。ｎ＝１の集約パケットには複数の個別パケットが含まれているわけではないが、便宜上集約パケットと称するものとする。なお、ｎは、１以上の自然数である。

【００５２】

図９に示すように、プロセッサー１１は、複数の個別パケット（ａ１）の集約、及び複数の個別パケット（ａ１）に対するヘッダーの付与を行うことで、集約パケット（ｂ１）を生成する。なお、個別パケット（ａ１）のそれぞれは、例えば、ペイロードである。ｎ個の個別パケットが集約された集約パケットは、集約ヘッダー、ｎ個の個別ヘッダー及びｎ個の個別パケットを含む。ｎ個の個別ヘッダー及びｎ個の個別パケットは、集約ヘッダーの後に続く。

集約ヘッダーは、集約パケットに含まれる個別パケットの数などの、集約パケット全体に関する情報を含む。

ｎ個の個別ヘッダーのそれぞれは、ｎ個の個別パケットのそれぞれに対して１対１で関連付けられる。すなわち、例えば、個別ヘッダーｋと個別パケットｋとが関連付けられる。ただし、ｋはｎ以下の自然数である。それぞれの個別ヘッダーは、集約パケットを個々の個別パケットに分割できるように、関連付けられた個別パケットのサイズなどの、関連付けられた個別パケットについての情報を含む。また、集約パケット（ｂ１）は、個別ヘッダーｋ、個別パケットｋ、個別ヘッダーｋ＋１、個別パケットｋ＋１、…のような順で、並んでいる。関連付けられた個別ヘッダーと個別パケットの組が隣り合うように並んでいる。

ステップＳ１５では、ｎ＝１であるため、ステップＳ１５で生成される集約パケットには、集約ヘッダー、個別ヘッダー１及び個別パケット１が含まれる。

【００５３】

ステップＳ１６においてプロセッサー１１（結合部１０４）は、集約バッファー１０２に未送信の個別パケットが記憶されているか否かを判定する。プロセッサー１１は、集約バッファー１０２に未送信の個別パケットが記憶されているならば、ステップＳ１６においてＹｅｓと判定してステップＳ１７へと進む。

【００５４】

ステップＳ１７においてプロセッサー１１（結合部１０４）は、集約パケットに次の個別パケットを結合した場合の集約パケットのデータ容量が、パケット処理装置１０が生成する集約パケットの最大データ容量以下となるか否かを判定する。なお、次の個別パケットとは、次に集約の対象となる個別パケットである。例えば、次の個別パケットは、集約バッファー１０２に記憶されている未送信の個別パケットの中で最初に記憶された個別パケットである。また、パケット処理装置１０が生成する集約パケットの最大データ容量は、例えば、パケット処理装置１０の管理者又は設計者などによって予め定められる。あるいは、パケット処理装置１０が生成する集約パケットの最大データ容量は、パケット処理装置１０が自動的に決定する。パケット処理装置１０が生成する集約パケットの最大データ容量は、パケット処理装置１０などのＭＴＵであっても良い。プロセッサー１１は、次の個別パケットを結合した場合の集約パケットのデータ容量が、当該集約パケットの最大データ容量以下となるならば、ステップＳ１７においてＹｅｓと判定してステップＳ１８へと進む。

【００５５】
ステップＳ１８においてプロセッサー１１（結合部１０４）は、集約バッファー１０２から次のパケットを取り出して、当該次のパケットを集約パケットに結合する。これにより、集約パケットに含まれる個別パケットの数が１つ増える。ここで、プロセッサー１１は、個別パケットを取り出すとき、集約バッファー１０２に記憶された当該個別パケットが送信済みであることが分かるようにする。あるいは、プロセッサー１１は、当該個別パケットを集約バッファーから削除する。
【００５６】
プロセッサー１１は、集約バッファー１０２に未送信の個別パケットが記憶されていないならば、ステップＳ１６においてＮｏと判定してステップＳ１９へと進む。また、プロセッサー１１は、次の個別パケットを結合した場合の集約パケットのデータ容量がパケット処理装置１０のＭＴＵを超えるならば、ステップＳ１７においてＮｏと判定してステップＳ１９へと進む。
かくして、プロセッサー１１は、集約バッファー１０２に未送信の個別パケットが記憶されていない状態になるか、次の個別パケットを結合した場合の集約パケットのデータ容量がパケット処理装置１０のＭＴＵを超えるまで、ステップＳ１６～ステップＳ１８を繰り返す。これにより、（ステップＳ１８の処理を行った回数＋１）個の個別パケットが集約された集約パケットが生成される。
【００５７】
ステップＳ１９においてプロセッサー１１（範囲選択部１０５）は、ステップＳ１５～ステップＳ１８の処理によって生成された集約パケットについて、暗号化する範囲を決定する。暗号化する範囲は、集約パケットのうちの暗号化されていない部分である。ステップＳ１９の処理は、範囲選択部１０５によって行われる。
ここで、個別パケットは、暗号化済みの場合と、平文の場合がある。したがって、暗号化済みの個別パケットに対してさらに暗号化すると、二重に暗号化されることとなってしまう。二重に暗号化した場合、二重に暗号化しなかった場合と比べて暗号化にかかる時間と復号にかかる時間が長くなり、また、処理負荷も大きくなる。このため、プロセッサー１１は、個別パケットについては、平文のもののみを暗号化することが好ましい。また、集約ヘッダー及び個別ヘッダーについては、ステップＳ１５又はステップＳ１８で付与したものであり、暗号化されていない。したがって、集約ヘッダー及び個別ヘッダーについては、暗号化することが好ましい。なお、プロセッサー１１は、それぞれの個別パケットが暗号化済みであるか否かについて、例えば、当該個別パケットの送信元であるクライアント装置３０から送信される情報により知ることができる。プロセッサー１１は、暗号化済みであるか否かが分からない個別パケットがある場合には、当該パケットを暗号化されているものとみなして暗号化しない。あるいは、プロセッサー１１は、暗号化済みであるか否かが分からない個別パケットがある場合には、当該パケットは暗号化されていないものとみなして暗号化する。あるいは、プロセッサー１１は、個別パケットが暗号化済みであるか否かの判定を行わずに、集約ヘッダー及び個別ヘッダーを含み、個別パケットを含まない範囲を暗号化の範囲として決定しても良い。これは、例えば、全ての個別パケットがクライアント装置３０などで暗号化されているような通信システム１において有用である。また、プロセッサー１１は、集約パケットに含まれる個別パケットのうちの暗号化済みのパケットが占める割合が予め定められた割合以下の場合には、暗号化済みの個別パケットを含めて集約パケット全体を暗号化しても良い。集約パケットに占める暗号化済みの個別パケットの割合が小さい場合には、集約パケット全体を暗号化した方が、集約パケットのうちの暗号化済みでない部分だけを暗号化するより負荷が小さくなる可能性がある。
以上より、プロセッサー１１は、暗号化前の集約パケットについて、集約ヘッダー、個別ヘッダー、及び平文の個別パケットを暗号化範囲として決定する。なお、図９には、暗号化済みである個別パケット１と、平文である個別パケット２を含む場合について例示している。したがって、図９に示す集約パケット（ｂ１）を暗号化する範囲は、集約ヘッダー、個別ヘッダー、及び個別パケット２を含む。

【００５８】
ステップＳ２０においてプロセッサー１１（暗号化部１０６）は、ステップＳ１９で決定した範囲を暗号化する。なお、プロセッサー１１は、暗号化する範囲以外については、暗号化の必要がないので、図９に示すようにコピーする。また、プロセッサー１１は、暗号化とともに、ＭＡＣ値の計算を行う。ＭＡＣ値の計算範囲は、例えば、暗号化の範囲であっても良いし、集約パケット全体であっても良い。また、プロセッサー１１は、集約前の個別パケットの一部又は全部にＭＡＣ値が付与されている場合には、暗号化の場合と同様に、ＭＡＣ値が付与されていない個別パケット、集約ヘッダー及び個別ヘッダーに対してＭＡＣ値の計算を行っても良い。
プロセッサー１１は、暗号化に、例えばＡＥＳ（Advanced Encryption Standard）又はその他の暗号を用いる。また、プロセッサー１１は、ＭＡＣ値の計算に、例えばＨＭＡＣ（hash-based message authentication code）、ＧＭＡＣ（Galois Message Authentication Code）又はその他のＭＡＣ値計算方法を用いる。また、プロセッサー１１は、暗号化の範囲とＭＡＣ値の計算範囲が同一の場合には、ＣＣＭ（Counter with CBC-MAC）、ＧＣＭ（Galois/Counter Mode）又はその他の認証付き暗号モードを用いることができる。認証付き暗号モードを用いることで、セキュリティ性の向上と、暗号化及びＭＡＣ値の計算の効率化とが期待できる。
なお、暗号化に利用する共通鍵又はＭＡＣ値の計算に利用する共通鍵は、例えば、通信セッションの確立時に鍵交換を行って共有しても良いし、予め各ノードの記憶装置に共通鍵を保存しておき、その鍵を利用しても良い。鍵交換を行う場合には、ディフィー・ヘルマン鍵交換又はその他の鍵交換方法を利用する。
なお、プロセッサー１１は、１つの集約パケット内における、パケット処理装置１０において暗号化する部分については、全て同一の暗号鍵を用いて良い。
ステップＳ１９及びステップＳ２０の処理が行われることで、集約パケットのうちの暗号化済みでないと判定された範囲が暗号化される。
【００５９】
以上より、集約される個別パケットに暗号化済みの個別パケットが含まれる場合、当該暗号化に使われた暗号鍵とパケット処理装置１０において暗号化された部分に使われた暗号鍵は異なることとなる。
【００６０】
ステップＳ２１においてプロセッサー１１（暗号化部１０６）は、暗号化情報を生成する。そして、プロセッサー１１は、生成した当該暗号化情報を集約パケットに付与する。
暗号化情報は、ＩＶ（initialization vector）、ＴＡＧ及びＳＩＺＥを含む。ＩＶは、ステップＳ１９の暗号化に用いられた初期化ベクトルである。ＴＡＧは、ステップＳ１９において求められたＭＡＣ値である。ＳＩＺＥは、暗号化情報の後に続くデータ範囲Ｒのデータサイズを示す。ただし、ＩＶを認証などの別の方法で交換する場合には、プロセッサー１１は、必ずしも毎回暗号化情報にＩＶを含める必要は無い。
ステップＳ１９～ステップＳ２１の処理によって、図９に示すように、暗号化前の集約パケット（ｂ１）に基づいて暗号化後の集約パケット（ｃ１）が生成される。
【００６１】
ステップＳ２２においてプロセッサー１１は、ステップＳ１５～ステップＳ２１の処理によって生成された暗号化後の集約パケットをサーバー装置２０に送信するように、第２の通信Ｉ／Ｆ１６（第１送信部１０７）に対して指示する。この指示を受けて第２の通信Ｉ／Ｆ１６は、当該集約パケットをサーバー装置２０に送信する。送信された当該集約パケットは、サーバー装置２０の通信Ｉ／Ｆ２５によって受信される。プロセッサー１１は、ステップＳ２２の処理の後、ステップＳ１１へと戻る。
【００６２】
一方、図６のステップＳ１０１においてサーバー装置２０のプロセッサー２１は、通信Ｉ／Ｆ２５によって集約パケットが受信されるのを待ち受けている。プロセッサー２１は、集約パケットが受信されたならば、ステップＳ１０１においてＹｅｓと判定してステップ

Ｓ１０２へと進む。
【００６３】
ステップＳ１０２においてプロセッサー２１は、ステップＳ１０１で受信された集約パケットを復号する。
ステップＳ１０３においてプロセッサー２１は、ステップＳ１０１で受信された集約パケットのＭＡＣ値を検証する。すなわち、プロセッサー２１は、集約パケットのＭＡＣ値を計算し、集約パケットに含まれるＭＡＣ値と一致するか否かを検証する。
なお、集約パケットが認証付き暗号モードで暗号化されている場合、プロセッサー２１は、ステップＳ１０２とステップＳ１０３を同時に行うこととなる。
【００６４】
ステップＳ１０４においてプロセッサー２１は、集約パケットのデータの完全性が保証されているか否かを判定する。プロセッサー２１は、ステップＳ１０３のＭＡＣ値の検証においてＭＡＣ値が一致したならば、ステップＳ１０４においてＮｏと判定してステップＳ１０５へと進む。
【００６５】
ステップＳ１０５においてプロセッサー２１は、集約パケットの各ヘッダーに含まれる情報などに基づき、集約パケットを個々の個別パケットに分割する。
【００６６】
ステップＳ１０６においてプロセッサー２１は、ステップＳ１０５において分割された個別パケットのそれぞれを処理バッファーに登録する。プロセッサー２１は、ステップＳ１０６の処理の後、ステップＳ１０１へと戻る。
【００６７】
対して、プロセッサー２１は、ステップＳ１０３のＭＡＣ値の検証においてＭＡＣ値が一致しなかったならば、ステップＳ１０４においてＹｅｓと判定してステップＳ１０７へと進む。例えば、集約パケットが改竄されていた場合など、データが書き換わっていた場合に、ＭＡＣ値が一致しなくなる。
ステップＳ１０７においてプロセッサー２１は、ステップＳ１０１で受信された集約パケットを破棄する。
【００６８】
ステップＳ１０８においてプロセッサー２１は、集約パケット全体の再送をパケット処理装置１０に要求する。プロセッサー２１は、ステップＳ１０８の処理の後、ステップＳ１０１へと戻る。
【００６９】
また、図７のステップＳ１１１においてプロセッサー２１は、処理バッファーに未処理パケットが記憶されているか否かを判定する。プロセッサー２１は、処理バッファーに未処理パケットが記憶されているならば、ステップＳ１１１においてＹｅｓと判定してステップＳ１１２へと進む。対して、プロセッサー２１は、処理バッファーに未処理パケットが記憶されていないならば、ステップＳ１１１においてＮｏと判定してステップＳ１１１を繰り返す。
【００７０】
ステップＳ１１２においてプロセッサー２１は、処理バッファーから未処理パケット１個を取り出し、当該未処理パケットに基づく処理を行う。プロセッサー２１は、未処理パケットを取り出すとき、処理バッファーに記憶された当該未処理パケットが処理済みであることが分かるようにする。あるいは、プロセッサー２１は、当該未処理パケットを処理バッファーから削除する。当該未処理パケットは、例えば、処理バッファーに記憶されている未処理パケットの中で最初に記憶された未処理パケットである。ここでの処理は、従来のサーバー装置が、クライアント装置３０から送信された、集約されていない状態の個別パケットを受信して、当該個別パケットに基づいて行う処理と同様である。
【００７１】
ステップＳ１１３においてプロセッサー２１は、ステップＳ１１２の処理内容に基づき、

必要に応じて、ステップＳ１１２で取り出した個別パケットの送信元であるクライアント装置３０に対して返信する応答を生成する。

【００７２】

ステップＳ１１４においてプロセッサー２１は、ステップＳ１１３において応答を生成した場合には、当該応答をパケットとしてサーバー集約バッファーに登録する。プロセッサー２１は、ステップＳ１１４の処理の後、ステップＳ１１１へと戻る。

【００７３】

また、図８のステップＳ１２１においてプロセッサー２１は、第２のタイマーをリセットする。第２のタイマーは、サーバー装置２０が前回集約パケットを送信してからの経過時間を計測するためのタイマーである。

【００７４】

ステップＳ１２２においてプロセッサー２１は、第２のタイマーをリセットしてから時間Ｔ２以上経過したか否かを判定する。なお、時間Ｔ２は、例えば、サーバー装置２０の管理者などによって予め設定される。あるいは、時間Ｔ２は、サーバー装置２０の設計者などによって予め定められていてもよい。プロセッサー２１は、第２のタイマーをリセットしてから時間Ｔ２が経過していないならば、ステップＳ１２２においてＮｏと判定してステップＳ１２３へと進む。

【００７５】

ステップＳ１２３においてプロセッサー２１は、サーバー集約バッファーに記憶された未送信の個別パケットのデータ容量の合計が容量Ｄ２以上であるか否かを判定する。なお、容量Ｄ２は、例えば、サーバー装置２０の管理者などによって予め設定される。あるいは、容量Ｄ２は、サーバー装置２０の設計者などによって予め定められていてもよい。容量Ｄ２は、例えば、サーバー装置２０が生成する集約パケットのＭＴＵである。プロセッサー２１は、サーバー集約バッファーに記憶された未送信の個別パケットのデータ容量の合計が容量Ｄ２以上でないならば、ステップＳ１２３においてＮｏと判定してステップＳ１２２へと戻る。かくして、プロセッサー２１は、第２のタイマーをリセットしてから時間Ｔ２が経過したか、サーバー集約バッファーに記憶された未送信の個別パケットのデータ容量の合計が容量Ｄ２以上となるまでステップＳ１２２及びステップＳ１２３を繰り返す。

【００７６】

プロセッサー２１は、ステップＳ１２２及びステップＳ１２３の待受状態にあるときに、第２のタイマーをリセットしてから時間Ｔ２が経過したならば、ステップＳ１２２においてＹｅｓと判定してステップＳ１２４へと進む。

【００７７】

ステップＳ１２４においてプロセッサー２１は、サーバー集約バッファーに未送信の個別パケットが記憶されているか否かを判定する。プロセッサー２１は、サーバー集約バッファーに未送信の個別パケットが記憶されていないならば、ステップＳ１２４においてＮｏと判定してステップＳ１２１へと戻る。すなわち、プロセッサー２１は、前回集約パケットを送信してから時間Ｔ２が経過しても未送信の個別パケットがサーバー集約バッファーに記憶されなかったならば、第２のタイマーをリセットする。対して、プロセッサー２１は、サーバー集約バッファーに未送信の個別パケットが記憶されているならば、ステップＳ１２４においてＹｅｓと判定してステップＳ１２５へと進む。

また、プロセッサー２１は、ステップＳ１２２及びステップＳ１２３の待受状態にあるときにサーバー集約バッファーに記憶された未送信の個別パケットのデータ容量の合計が容量Ｄ２以上であるならば、ステップＳ１２３においてＹｅｓと判定してステップＳ１２５へと進む。

【００７８】

ステップＳ１２５においてプロセッサー２１は、サーバー集約バッファーに記憶された未送信の個別パケット１個を取り出す。ここで、プロセッサー２１は、個別パケットを取り出すとき、サーバー集約バッファーに記憶された当該個別パケットが送信済みであることが分かるようにする。あるいは、プロセッサー２１は、当該個別パケットをサーバー集約

バッファーから削除する。当該個別パケットは、例えば、サーバー集約バッファーに記憶されている未送信の個別パケットの中で最初に記憶された個別パケットである。ここで生成される集約パケットは、パケット処理装置１０が図４のステップＳ１５で生成するものと同様のものである。

【００７９】

図８のステップＳ１２６においてプロセッサー２１は、サーバー集約バッファーに未送信の個別パケットが記憶されているか否かを判定する。プロセッサー２１は、サーバー集約バッファーに未送信の個別パケットが記憶されているならば、ステップＳ１２６においてＹｅｓと判定してステップＳ１２７へと進む。

【００８０】

ステップＳ１２７においてプロセッサー２１は、集約パケットに次の個別パケットを結合した場合の集約パケットのデータ容量が、サーバー装置２０が生成する集約パケットの最大データ容量以下となるか否かを判定する。なお、次の個別パケットとは、次に集約の対象となる個別パケットである。例えば、次の個別パケットは、サーバー集約バッファーに記憶されている未送信の個別パケットの中で最初に記憶された個別パケットである。また、サーバー装置２０が生成する集約パケットの最大データ容量は、例えば、サーバー装置２０の管理者又は設計者などによって予め定められる。あるいは、サーバー装置２０が生成する集約パケットの最大データ容量は、サーバー装置２０が自動的に決定する。サーバー装置２０が生成する集約パケットの最大データ容量は、サーバー装置２０のＭＴＵであっても良い。プロセッサー２１は、次の個別パケットを結合した場合の集約パケットのデータ容量が、サーバー装置２０が生成する集約パケットの最大データ容量以下となるならば、ステップＳ１２７においてＹｅｓと判定してステップＳ１２８へと進む。

【００８１】

ステップＳ１２８においてプロセッサー２１は、サーバー集約バッファーから次のパケットを取り出して、当該次のパケットを集約パケットに結合する。これにより、集約パケットに含まれる個別パケットの数が１つ増える。ここで、プロセッサー２１は、個別パケットを取り出すとき、サーバー集約バッファーに記憶された当該個別パケットが送信済みであることが分かるようにする。あるいは、プロセッサー２１は、当該個別パケットを集約バッファーから削除する。

【００８２】

プロセッサー２１は、サーバー集約バッファーに未送信の個別パケットが記憶されていないならば、ステップＳ１２６においてＮｏと判定してステップＳ１２９へと進む。また、プロセッサー２１は、次の個別パケットを結合した場合の集約パケットのデータ容量がサーバー装置２０のＭＴＵを超えるならば、ステップＳ１２７においてＮｏと判定してステップＳ１２９へと進む。

かくして、プロセッサー２１は、サーバー集約バッファーに未送信の個別パケットが記憶されていない状態になるか、次の個別パケットを結合した場合の集約パケットのデータ容量がサーバー装置２０のＭＴＵを超えるまで、ステップＳ１２６～ステップＳ１２８を繰り返す。これにより、（ステップＳ１２８の処理を行った回数＋１）個の個別パケットが集約された集約パケットが生成される。

【００８３】

ステップＳ１２９においてプロセッサー２１は、ステップＳ１２５～ステップＳ１２８の処理によって作成された集約パケットについて、暗号化する範囲を決定する。プロセッサー２１は、暗号化範囲の決定を、パケット処理装置１０のプロセッサー１１が図４のステップＳ１９で行うものと同様にして行う。

【００８４】

図８のステップＳ１３０においてプロセッサー２１は、ステップＳ１２９で決定した範囲を暗号化する。プロセッサー２１は、暗号化を、パケット処理装置１０のプロセッサー１１が図４のステップＳ２０で行うものと同様にして行う。

ステップＳ１２９及びステップＳ１３０の処理が行われることで、集約パケットのうちの

暗号化済みでないと判定された範囲が暗号化される。
【００８５】
図８のステップＳ１３１においてプロセッサー２１は、暗号化情報を生成する。そして、プロセッサー２１は、生成した当該暗号化情報を集約パケットに付与する。プロセッサー２１は、暗号化情報の生成を、パケット処理装置１０のプロセッサー１１が図４のステップＳ２１で行うものと同様にして行う。
【００８６】
図８のステップＳ１３２においてプロセッサー２１は、ステップＳ１２５～ステップＳ１３１の処理によって作成された集約パケットをパケット処理装置１０に送信するように、通信Ｉ／Ｆ２５に対して指示する。この指示を受けて通信Ｉ／Ｆ２５は、当該集約パケットをパケット処理装置１０に送信する。送信された当該集約パケットは、パケット処理装置１０の第２の通信Ｉ／Ｆ１６によって受信される。プロセッサー２１は、ステップＳ１３２の処理の後、ステップＳ１２１へと戻る。
【００８７】
一方、図５のステップＳ３１においてパケット処理装置１０のプロセッサー１１は、通信Ｉ／Ｆ２５（第２受信部１０８）によって集約パケットが受信されるのを待ち受けている。プロセッサー１１は、集約パケットが受信されたならば、ステップＳ３１においてＹｅｓと判定してステップＳ３２へと進む。
【００８８】
ステップＳ３２においてプロセッサー１１（復号部１０９）は、ステップＳ３１で受信された集約パケットを復号する。
ステップＳ３３においてプロセッサー１１（復号部１０９）は、ステップＳ３１で受信された集約パケットのＭＡＣ値を検証する。すなわち、プロセッサー１１は、集約パケットのＭＡＣ値を計算し、集約パケットに含まれるＭＡＣ値と一致するか否かを検証する。
なお、集約パケットが認証付き暗号モードで暗号化されている場合、プロセッサー１１は、ステップＳ３２とステップＳ３３を同時に行うこととなる。
【００８９】
ステップＳ３４においてプロセッサー１１（復号部１０９）は、集約パケットのデータの完全性が保証されているか否かを判定する。プロセッサー１１は、ステップＳ３３のＭＡＣ値の検証においてＭＡＣ値が一致したならば、ステップＳ３４においてＮｏと判定してステップＳ３５へと進む。
【００９０】
ステップＳ３５においてプロセッサー１１（分割部１１０）は、集約パケットの各ヘッダーに含まれる情報などに基づき、集約パケットを個々の個別パケットに分割する。
【００９１】
ステップＳ３６においてプロセッサー１１は、ステップＳ３５において分割された個別パケットのそれぞれを、それぞれの個別パケットの宛先であるクライアント装置３０に送信するように第１の通信Ｉ／Ｆ１５（第２送信部１１１）に対して指示する。この指示を受けて第１の通信Ｉ／Ｆ１５は、当該個別パケットをそれぞれの個別パケットの宛先であるクライアント装置３０に送信する。プロセッサー１１は、ステップＳ３６の処理の後、ステップＳ３１へと戻る。
【００９２】
対して、プロセッサー１１は、ステップＳ３３のＭＡＣ値の検証においてＭＡＣ値が一致しなかったならば、ステップＳ３４においてＹｅｓと判定してステップＳ３７へと進む。例えば、集約パケットが改竄されていた場合など、データが書き換わっていた場合に、ＭＡＣ値が一致しなくなる。
ステップＳ３７においてプロセッサー１１は、ステップＳ３１で受信された集約パケットを破棄する。
【００９３】
ステップＳ３８においてプロセッサー１１は、集約パケットの再送をサーバー装置２０に

要求する。プロセッサー１１は、ステップＳ３８の処理の後、ステップＳ３１へと戻る。
【００９４】
第１実施形態の通信システム１によれば、パケット通信装置１０及びサーバー装置２０は、複数の個別パケットを集約する。これにより、パケット通信装置１０の第２の通信Ｉ／Ｆ１６とサーバー装置２０の通信Ｉ／Ｆ２５にかかる負荷が低減される。
また、第１実施形態の通信システム１によれば、パケット通信装置１０及びサーバー装置２０は、集約パケットを暗号化する。これにより、集約プロトコルに付与されるヘッダー情報などの盗聴を防止することができる。また、第１実施形態の通信システム１によれば、パケット通信装置１０及びサーバー装置２０は、集約パケットにＭＡＣ値を付与する。これにより、集約パケットのデータの完全性の検証が可能となる。
さらに、第１実施形態の通信システム１によれば、パケット通信装置１０及びサーバー装置２０は、暗号化済みの部分を除いて集約パケットを暗号化する。このため、パケット通信装置１０及びサーバー装置２０は、全体を暗号化する場合に比べて暗号化にかかる時間と復号に係る時間とを低減することができる。これにより、クライアント装置３０とサーバー装置２０との間のやり取りのリアルタイム性が向上する。
以上より、第１実施形態の通信システム１は、図９の（ｃ１）に示すような集約パケットを用いることで、最低限の負荷で情報の漏洩防止やデータの改竄の検出を行うことが可能となる。また、暗号化及び復号にかかる時間を最小限にすることで、通信のリアルタイム性低下を防ぐことができる。
【００９５】
クライアント装置３０が駅務装置である場合、クライアント装置３０から送信されるリクエストとサーバー装置２０から送信されるレスポンスは、データ量が小さく、データの送受信回数も多い。また、自動改札機などでは、特にリアルタイム性が要求される。さらに、クライアント装置３０として駅務装置を含む通信システム１では、通信内容に、金銭に関する情報及び個人情報なども含まれるため、送信されるデータの改竄及び盗聴を防ぐ必要がある。以上より、クライアント装置３０が駅務装置を含む場合、実施形態の通信システム１は特に有用である。なお、自動改札機が送信する情報は、一例として、入場駅情報、出場駅情報、入場時間、出場時間、ＩＣカードの認証情報、金額情報又はこれらのうちの複数などを含む。
【００９６】
〔第２実施形態〕
第２実施形態の通信システム１の構成は、第１実施形態と同様であるので説明を省略する。また、第２実施形態の通信システム１のパケット通信装置１０及びサーバー装置２０の動作は、第１実施形態と同様であるので説明を省略する。ただし、第２実施形態では、生成される集約パケットが第１実施形態とは異なる。以下、第２実施形態において生成される集約パケットについて図１０に基づいて説明する。図１０は、第２実施形態に係る集約パケットの一例を説明するための図である。なお、図１０において第１実施形態の図２と同様の要素については同一の符号を付している。図１０における図２と同様の要素については説明を省略する場合がある。
【００９７】
図１０には、暗号化済みである個別パケット１及び個別パケット３と、平文である個別パケット２及び個別パケット４とを含むｎ個の個別パケットを集約する場合について例示している。第２実施形態の集約パケットは、（ｂ２）に示すように、集約ヘッダー、ｎ個の個別ヘッダー、平文の個別パケット、暗号化済みの個別パケットの順でデータが並んでいる。すなわち、集約パケット（ｂ２）は、暗号化済みでない部分が連続した後に、暗号化済みである部分が連続するような並びである。このように、暗号化済みでないデータが連続して並んでいることで、プロセッサー１１及びプロセッサー２１は、集約ヘッダー、ｎ個の個別ヘッダー及び平文の個別パケットを一度に暗号化することができる。さらに、暗号化済みであるデータが連続して並んでいることで、プロセッサー１１及びプロセッサー２１は、暗号化済みの個別パケットを一度にコピーすることができる。

【００９８】
第２実施形態の通信システム１によれば、第１実施形態と同様の効果が得られる。
また、第２実施形態の通信システム１によれば、またＣＢＣなど、暗号の利用モードによっては暗号化されるデータが分散すると、ブロック長に満たない部分をパディングで埋める必要があり、実装方法によっては個別ヘッダーごとにパディングが発生する可能性がある。特に、個々の個別パケットサイズが小さい場合、集約パケット全体にパディングが占める割合が大きくなり、集約パケットのデータサイズが大きくなってしまう。そこで、第２実施形態のように暗号化対象のデータを集約パケット中の一か所にまとめて集約パケットを構成することで、集約パケットのデータサイズの増大を防ぐことができる。また、一度に暗号化及び復号を行うことができるので、処理速度の向上が見込める。したがって、第２実施形態の通信システム１は、図１０に（ｂ２）及び（ｃ２）に示すような集約パケットを用いることで、リアルタイム性を向上させることができる。
【００９９】
〔第３実施形態〕
第２実施形態の通信システム１の構成は、第１実施形態と同様であるので説明を省略する。ただし、第２実施形態のＲＡＭ１３又は補助記憶デバイス１４は、再送リスト及び受信済みリストを記憶する。再送リストは、パケット処理装置１０が再送を要求する個別パケットのリストである。再送リストは、例えば、再送を要求する個別パケットのそれぞれに関連付けられたシーケンス番号を記憶することで、当該個別パケットを登録する。受信済みリストは、パケット処理装置１０に正常に到着した個別パケットのリストである。受信済みリストは、例えば、正常に到着した個別パケットのそれぞれに関連付けられたシーケンス番号を記憶することで、当該個別パケットを登録する。シーケンス番号は、個別パケットごとにユニークに付与される識別子の一例である。
また、第３実施形態のパケット集約装置は、図２に代えて図１１に示すような機能構成である。図１１は、第３実施形態に係るパケット処理装置１０の機能構成を示すブロック図である。第３実施形態に係るパケット処理装置１０は、第１受信部１０１、集約バッファー１０２、周期管理部１０３、結合部１０４、範囲選択部１０５、第１送信部１０７、第２受信部１０８、分割部１１０、第２送信部１１１、冗長化部１２１、到着管理部１２２、再送要求部１２３、暗号化部１２４及び復号部１２５を含む。
【０１００】
冗長化部１２１は、暗号化された集約パケットを複数回送信するために、結合部１０４から渡された集約パケットを複製する機能を有する。そして、冗長化部１２１は、第１送信部１０７に集約パケットを複数回渡して、複数回送信を依頼する機能を有する。例えば、プロセッサー１１が冗長化部１２１として機能する。
【０１０１】
到着管理部１２２は、パケットの到着回数を管理する機能を有し、クライアント装置３０に個別パケットを送信するか判断する機能を有する。到着管理部１２２は、復号部１２５から渡された個別パケットのシーケンス番号などの識別子を用いて個別パケットの到着回数を管理する。そして、到着管理部１２２は、個別パケットが初めて到着した際には第２送信部１１１を呼び出してクライアント装置３０に当該個別パケットを送信する。一方で、到着管理部１２２は、２度目以降の個別パケットの到着では、当該個別パケットを破棄する。これにより、複数回送信された集約パケットに含まれる個別パケットのうち、最初に到着した個別パケットのみをクライアント装置３０に送信することができる。また、到着管理部１２２は、個別パケットの識別子から個別パケットの消失を検出する機能も有する。すなわち、例えば、到着管理部１２２は、個別パケットの識別子としてシーケンス番号を利用する場合には、シーケンス番号の数字が飛んだ場合には、飛んだ数字に対応する個別パケットが消失したと判定する。例えば、到着管理部１２２は、到着した個別パケットのシーケンス番号が１，２，４である場合には、飛んでいるシーケンス番号３の個別パケットが消失したと判定する。そして、到着管理部１２２は、例えば、再送要求部１２３に、飛んでいるシーケンス番号を再送リストへ登録するように要求する。そして、到着管

理部１２２は、飛んでいるシーケンス番号の個別パケットが後から到着した際には、当該飛んでいるシーケンス番号を再送リストから削除するように再送要求部１２３に要求する。例えば、プロセッサー１１が到着管理部１２２として機能する。

【０１０２】

再送要求部１２３は、集約バッファー１０２に再送要求用のパケットを登録する機能を有する。例えば、再送要求部３０２は、再送リストで指定されている個別パケットを一定間隔ごとに全て再送要求する。あるいは、再送要求部１２３は、再送リストに登録されている個別パケットごとに、再送要求を送信させた回数に応じて再送要求する間隔を変化させても良い。例えば、再送要求部１２３は、再送要求のパケットが送信された回数が０回の個別パケットについては、到着した個別パケットの番号が飛んでいることが検出されたらすぐに再送要求を送信させる。そして、再送要求部１２３は、再送要求を送信させた回数が多いほど、次に再送要求を送信させるまでの時間を長くする。また、再送要求部１２３は、再送リストが溢れることを防ぐため、一定回数再送要求を送っても到着しない個別パケットについては、再送リストから登録解除しても良い。あるいは、再送要求部１２３は、再送リストが溢れそうになるたびに、再送リストに登録された個別パケットを、登録が古い順から登録解除しても良い。あるいは、再送要求部１２３は、再送リストが溢れそうになるたびに、登録されている中でシーケンス番号が最も若い個別パケットを、登録解除しても良い。例えば、プロセッサー１１が再送要求部１２３として機能する。

【０１０３】

また、最新のシーケンス番号のパケットが消失した場合にも再送要求を送信するため、到着管理部１２２は、定期的に、サーバー装置２０から、送信済みの個別パケットの最大のシーケンス番号を取得する。そして、到着管理部１２２は、取得したシーケンス番号が、到着済みの個別パケットのうちの最大のシーケンス番号よりも大きいか否かを判定する。そして、到着管理部１２２は、サーバー装置２０から取得したシーケンス番号の方が大きい場合には、到着済みの個別パケットのうちの最大のシーケンス番号＋１～取得したシーケンス番号を再送リストに登録させるように再送要求部１２３に要求する。

【０１０４】

また、再送要求部１２３は、サーバー装置２０から明示的に再送要求のパケットを受け付ける機能を持っていても良い。再送要求部１２３は、当該再送要求のパケットを受け付けた場合、集約バッファー１０２に含まれる送信済みのパケットを再度送信するようにフラグ設定する。これにより、周期管理部１０３は、集約バッファー１０２からサーバー装置２０に送信するパケットを取り出す際に、当該フラグが設定されたパケットを取り出すようになる。したがって、周期管理部１０３は、サーバー装置２０の要求に応じたパケットの再送が可能となる。

【０１０５】

暗号化部１２４は、第１実施形態とは異なる後述するような方法で集約パケットの暗号化及び複数のＭＡＣ値の付与などを行う機能を有する。

【０１０６】

復号部１２５は、集約パケットに含まれる複数のＭＡＣ値ごとにデータの完全性を検証する機能を有する。また、復号部１２５は、集約パケットの暗号化された部分を復号する。そして、復号部１２５は、集約ヘッダーに改竄が検出された場合には、集約パケット全体を破棄する機能を有する。また、復号部１２５は、集約パケットに含まれる個別パケットのうちの改竄が検出された個別パケットを破棄する。そして、復号部１２５は、改竄が検出されなかった個別パケットについては、到着管理部１２２に渡す。

【０１０７】

以下、第３実施形態に係る通信システム１の動作を図１２及び図１３に基づいて説明する。なお、以下の動作説明における処理の内容は一例であって、同様な結果を得ることが可能な様々な処理を適宜に利用できる。図１２及び図１３は、パケット処理装置１０のプロセッサー１１による処理のフローチャートである。

【０１０８】

第３実施形態では、パケット処理装置１０は、第１実施形態と同様に図３及び図４に示す処理と同様の処理により、集約パケットの生成及び送信などを行う。また、サーバー装置２０は、第１実施形態と同様に図７及び図８に示す処理と同様の処理により、集約パケットの生成及び送信などを行う。ただし、第３実施形態では、生成される集約パケットが、第１実施形態及び第２実施形態とは異なる。第３実施形態において生成される集約パケットについて図１４に基づいて説明する。図１４は、第３実施形態に係る集約パケットの一例を説明するための図である。

【０１０９】

図１４には、暗号化済みである個別パケット１と、平文である個別パケット２とを含むｎ個の個別パケットを集約する場合について例示している。第３実施形態の集約パケットの集約ヘッダー、個別ヘッダー及び個別パケットの順序は、例えば、（ｂ３）及び（ｃ３）に示すように第１実施形態と同様である。すなわち、個別パケットそれぞれに対して、個別パケット単位で暗号化が行われる。

ただし、第３実施形態の暗号化後の集約パケットは（ｃ３）は、暗号化情報として、複数のＭＡＣ値を含む。プロセッサー１１又はプロセッサー２１は、これら複数のＭＡＣ値を、集約パケットのうちの改竄検出を行いたい単位でそれぞれ計算及び付与を行う。例えば、第３実施形態の暗号化後の集約パケット（ｃ３）は、暗号化情報として、例えば、ＩＶ、ＴＡＧＡ、ＴＡＧ０、ＴＡＧ１、ＴＡＧ２、…ＴＡＧｎ及びＳＩＺＥを含む。

ＴＡＧＡは、集約パケット全体に対するＭＡＣ値である。

ＴＡＧ０は、集約ヘッダーに対するＭＡＣ値である。

ＴＡＧｋ（ｋは、ｎ以下の自然数）は、個別ヘッダーｋと個別パケットｋとの組のＭＡＣ値である。なお、個別パケットｋに既にＭＡＣ値が付与されている場合には、ＴＡＧｋは、個別ヘッダーｋのＭＡＣ値であっても良い。すなわち、ＴＡＧ１～ｎは、個別パケット単位で付与されるＭＡＣ値である。

単位でＭＡＣ値の付与が行われている。

なお、プロセッサー１１（暗号化部１２４）又はプロセッサー２１は、集約パケットに含まれる一部の個別パケットが改竄された場合に、別の個別パケットの復号を可能とするため、ＭＡＣ値の計算と暗号化を同じ単位で行う事が好ましい。あるいは、プロセッサー１１（暗号化部１２４）又はプロセッサー２１は、集約パケットに含まれる一部の個別パケットが改竄された場合に、別の個別パケットの復号を可能とするため、ＣＴＲ（Counter）モードなどの、ブロックごとに独立で復号でき、他のブロックの改ざんが復号結果に影響しない暗号利用モードを用いる。これは、集約パケット全体をＣＢＣモードなど、暗号化がチェインするモードで復号すると、前ブロックの改竄が後ろのブロックの復号結果に影響するためである。また、プロセッサー１１（暗号化部１２４）又はプロセッサー２１は、集約パケット内に含まれる個別パケットを識別し、個々の個別パケット毎に再送などの処理を行えるようにするため、個別ヘッダーにシーケンス番号などの識別子を含めることが好ましい。このシーケンス番号は、集約パケット毎にリセットせず、インクリメントする。例えば、１番目の集約パケットにシーケンス番号１，２，３の個別パケットが含まれた場合には、次の集約パケットである２番目の集約パケットに含まれるパケットのシーケンス番号は、４から開始することとなる。

【０１１０】

また、第３実施形態では、パケット処理装置１０及びサーバー装置２０は、図４のステップＳ２２又は図８のステップＳ１３２において、同一の集約パケットを複数回送信する。送信回数は、例えば２回である。なお、パケット処理装置１０及びサーバー装置２０は、集約パケットの送信元から送信先までの経路が複数ある場合には、送信ごとに異なる経路を通じて同一の集約パケットを送信しても良い。

【０１１１】

図１２のステップＳ４１においてパケット処理装置１０のプロセッサー１１は、第２の通信Ｉ／Ｆ１６（第２受信部１０８）によって集約パケットが受信されるのを待ち受けている。プロセッサー１１は、集約パケットが受信されたならば、ステップＳ４１においてＹ

ｅｓと判定してステップＳ４２へと進む。
【０１１２】
ステップＳ４２においてプロセッサー１１（復号部１２５）は、集約パケット全体のＭＡＣ値であるＴＡＧＡを検証する。すなわち、プロセッサー１１は、ステップＳ４１で受信された集約パケット全体のＭＡＣ値を計算し、当該集約パケットに含まれるＴＡＧＡと一致するか否かを検証する。
【０１１３】
ステップＳ４３においてプロセッサー１１（復号部１２５）は、ステップＳ４１で受信された集約パケット全体のデータの完全性が保証されているか否かを判定する。プロセッサー１１は、ステップＳ４３のＭＡＣ値の検証においてＭＡＣ値が一致したならば、ステップＳ４３においてＮｏと判定してステップＳ４４へと進む。
【０１１４】
ステップＳ４４においてプロセッサー１１（分割部１１０）は、ステップＳ４１で受信された集約パケットを個々の個別ヘッダーと個別パケットとの組に分割する。ここで、個別ヘッダーと個別パケットとの組とは、例えば、個別ヘッダー１と個別パケット１との組、個別ヘッダー２と個別パケット２との組、又は個別ヘッダーｎと個別パケットｎとの組などである。
【０１１５】
ステップＳ４５においてプロセッサー１１（復号部１２５）は、ステップＳ４４で分割された個別ヘッダーと個別パケットとの組それぞれを復号する。
【０１１６】
対して、プロセッサー１１は、ステップＳ４３のＭＡＣ値の検証においてＭＡＣ値が一致しなかったならば、ステップＳ４３においてＹｅｓと判定してステップＳ４６へと進む。例えば、ステップＳ４１で受信された集約パケットが改竄されていた場合など、データが書き換わっていた場合に、ＭＡＣ値（ＴＡＧＡ）が一致しなくなる。
ステップＳ４６においてプロセッサー１１（復号部１２５）は、集約ヘッダーを復号する。
【０１１７】
ステップＳ４７においてプロセッサー１１（復号部１２５）は、集約ヘッダーのＭＡＣ値を検証する。すなわち、プロセッサー１１は、集約ヘッダーのＭＡＣ値を計算し、ステップＳ４１で受信された集約パケットに含まれるＴＡＧ０と一致するか否かを検証する。
【０１１８】
ステップＳ４８においてプロセッサー１１（復号部１２５）は、集約ヘッダーのデータの完全性が保証されているか否かを判定する。プロセッサー１１は、ステップＳ４７のＭＡＣ値の検証においてＭＡＣ値が一致したならば、ステップＳ４８においてＮｏと判定してステップＳ４９へと進む。
【０１１９】
ステップＳ４９においてプロセッサー１１（分割部１１０）は、ステップＳ４１で受信された集約パケットを個々の個別ヘッダーと個別パケットとの組に分割する。
【０１２０】
ステップＳ５０においてプロセッサー１１（復号部１２５）は、ステップＳ４９で分割された個別ヘッダーと個別パケットとの組それぞれを復号する。
【０１２１】
ステップＳ５１においてプロセッサー１１（復号部１２５）は、個別ヘッダーと個別パケットとの組それぞれについて、ＭＡＣ値を検証する。すなわち、プロセッサー１１は、個別ヘッダーと個別パケットとの組それぞれについてＭＡＣ値を計算し、対応するそれぞれの個別ヘッダーと個別パケットとの組についてのＴＡＧと一致するか否かを検証する。
【０１２２】
ステップＳ５２においてプロセッサー１１（復号部１２５）は、集約ヘッダーのデータの完全性が保証されていない個別ヘッダーと個別パケットとの組を破棄する。すなわち、プロセッサー１１は、ステップＳ５１においてＭＡＣ値が一致しなかった個別ヘッダーと個

別パケットとの組を破棄する。例えば、個別ヘッダー又は個別パケットが改竄されていた場合など、データが書き換わっていた場合に、対応するＭＡＣ値（ＴＡＧ１～ＴＡＧｎ）が一致しなくなる。

【０１２３】

プロセッサー１１は、ステップＳ４５又はステップＳ５２の処理の後、ステップＳ５３へと進む。

ステップＳ５３においてプロセッサー１１（到着管理部１２２）は、ステップＳ４５又はステップＳ５０で復号した個別パケットのうち、受信済みの個別パケットを破棄する。

【０１２４】

ステップＳ５４においてプロセッサー１１（再送要求部１２３及び到着管理部１２２）は、再送リスト及び受信済みリストを更新する。すなわち、プロセッサー１１は、ステップＳ４５又はステップＳ５０で復号した個別パケットのうち、ステップＳ５２及びステップＳ５３のいずれにおいても破棄されなかった個別パケットのシーケンス番号を受信済みリストに登録する。また、プロセッサー１１は、受信済みリストに登録したシーケンス番号と同一のシーケンス番号が再送リストに登録されている場合には、当該シーケンス番号を再送リストから削除する。さらに、プロセッサー１１は、ステップＳ５０で復号した個別パケットのうち、ステップＳ５２で破棄した個別パケットのシーケンス番号が、受信済みリストに登録されていない場合には、当該シーケンス番号を再送リストに登録する。また、プロセッサー１１は、受信済みリストに登録された最大のシーケンス番号未満のシーケンス番号のうち、再送リストにも受信済みリストにも登録されていないシーケンス番号がある場合には、当該シーケンス番号を再送リストに登録する。加えて、プロセッサー１１は、サーバー装置２０から、送信済みの個別パケットの最大シーケンス番号を取得しても良い。そして、プロセッサー１１は、サーバー装置２０から取得した最大シーケンス番号以下のシーケンス番号のうち、再送リストにも受信済みリストにも登録されていないシーケンス番号がある場合には、当該シーケンス番号を再送リストに登録する。

【０１２５】

ステップＳ５５においてプロセッサー１１（再送要求部１２３）は、ステップＳ４５又はステップＳ５０で復号した個別パケットのうち、ステップＳ５２及びステップＳ５３のいずれにおいても破棄されなかった個別パケットのそれぞれを、それぞれの個別パケットの宛先であるクライアント装置３０に送信するように第１の通信Ｉ／Ｆ１５（第２送信部１１１）に対して指示する。この指示を受けて第１の通信Ｉ／Ｆ１５は、当該個別パケットのそれぞれを、それぞれの個別パケットの宛先であるクライアント装置３０に送信する。送信された当該個別パケットは、それぞれ宛先であるクライアント装置３０の通信Ｉ／Ｆ３５によって受信される。プロセッサー１１は、ステップＳ５５の処理の後、ステップＳ４１へと戻る。

【０１２６】

対して、プロセッサー１１は、ステップＳ４３のＭＡＣ値の検証においてＭＡＣ値が一致しなかったならば、ステップＳ４８においてＹｅｓと判定してステップＳ５６へと進む。例えば、集約ヘッダーが改竄されていた場合など、データが書き換わっていた場合に、ＭＡＣ値（ＴＡＧ０）が一致しなくなる。

ステップＳ５６においてプロセッサー１１（復号部１２５）は、ステップＳ４１で受信された集約パケットを破棄する。

【０１２７】

ステップＳ５７においてプロセッサー１１（再送要求部１２３及び到着管理部１２２）は、再送リストを更新する。すなわち、プロセッサー１１は、ステップＳ５６で破棄した集約パケットに含まれる個別パケットのシーケンス番号が、受信済みリストに登録されていない場合には、当該シーケンス番号を再送リストに登録する。また、プロセッサー１１は、サーバー装置２０から、送信済みの個別パケットの最大シーケンス番号を取得しても良い。そして、プロセッサー１１は、サーバー装置２０から取得した最大シーケンス番号以下のシーケンス番号のうち、再送リストにも受信済みリストにも登録されていないシーケ

ンス番号がある場合には、当該シーケンス番号を再送リストに登録する。プロセッサー１１は、ステップＳ５７の処理の後、ステップＳ４１へと戻る。

【０１２８】

また、図１３のステップＳ６１においてプロセッサー１１は、第３のタイマーをリセットする。第３のタイマーは、パケット処理装置１０が前回再送要求パケットを集約バッファー１０２に登録してからの経過時間を計測するためのタイマーである。

【０１２９】

ステップＳ６２においてプロセッサー１１は、第３のタイマーをリセットしてから時間Ｔ３以上経過するのを待ち受ける。なお、時間Ｔ３は、例えば、パケット処理装置１０の管理者などによって予め設定される。あるいは、時間Ｔ３は、パケット処理装置１０の設計者などによって予め定められていてもよい。プロセッサー１１は、第３のタイマーをリセットしてから時間Ｔ３以上経過したならば、ステップＳ６２においてＹｅｓと判定してステップＳ６３へと進む。

【０１３０】

ステップＳ６３においてプロセッサー１１は、サーバー装置２０を宛先とする再送要求パケットを集約バッファー１０２に登録する。再送要求パケットには、例えば、再送リストに登録されたシーケンス番号が含まれる。なお、プロセッサー１１は、例えば、再送要求パケットを個別パケットとして集約バッファー１０に登録する。したがって、再送要求パケットは、集約バッファー１０に登録された他の個別パケットとともに集約されて、集約パケットに含まれる。そして、当該再送要求パケットは、集約パケットに含まれた状態でサーバー装置２０に送信される。プロセッサー１１は、ステップＳ６３の処理の後、ステップＳ６１へと戻る。

一方、再送要求パケットは、サーバー装置２０のプロセッサー２１によって処理バッファーに登録される。そして、プロセッサー２１は、図７のステップＳ１１２において処理バッファーに登録された再送要求パケットに基づき、当該再送要求パケットに含まれるシーケンス番号で特定される個別パケットをサーバー集約バッファーに登録する。例えば、プロセッサー２１は、サーバー集約バッファーに当該個別パケットが送信済み状態として記憶されている場合には、当該個別パケットを未送信状態に戻す。あるいは、プロセッサー２１は、サーバー集約バッファーに当該個別パケットが記憶されていない場合には、当該個別パケットをサーバー集約バッファーに記憶させる。なお、プロセッサー２１は、次の個別パケットとして、サーバー集約バッファーに記憶されている未送信の個別パケットの中で最もシーケンス番号が若いものを選択しても良い。

【０１３１】

また、サーバー装置２０についても、プロセッサー２１は、図１２及び図１３に示す処理と同様の処理により、集約パケットの復号、分割、ＭＡＣ検証及び再送要求などを行う。また、パケット処理装置１０についても、サーバー装置２０と同様に、サーバー装置２０から再送要求パケットを受け取った場合には、当該再送要求パケットに含まれるシーケンス番号で特定される個別パケットを、サーバー装置２０が再送要求パケットを受け取った場合の処理と同様の処理を行うことで、サーバー装置２０に再送する。

【０１３２】

以上説明したようなパケット処理装置１０及びサーバー装置２０の処理により行われる通信を、一例を挙げて図１５を用いて説明する。図１５は、第３実施形態に係る通信システム１の情報の流れの一例を示すシーケンス図である。

【０１３３】

ステップＳＴ１においてサーバー装置２０は、集約パケットをパケット処理装置１０に送信する。なお、当該集約パケットには、一例として、シーケンス番号１～６の６つの個別パケットが含まれるものとする。また、サーバー装置２０は、一例として、当該集約パケットを２回、パケット処理装置１０に送信するものとする。

【０１３４】

パケット処理装置１０は、サーバー装置２０がステップＳＴ１で２回送信した集約パケッ

トを受信する。ここで、ステップＳＴ１の１回目に送信された集約パケットのうち、シーケンス番号４番と５番の個別パケットが改竄されていたものとする。パケット処理装置１０は、ＭＡＣ値の検証により、この改竄を検出することができる。したがって、パケット処理装置１０は、ステップＳＴ１の１回目に送信された集約パケットのうち、シーケンス番号４番と５番の個別パケットを破棄する。また、ステップＳＴ１の２回目に送信された集約パケットのうち、シーケンス番号が３番と５番の個別パケットが改竄されていたものとする。パケット処理装置１０は、ＭＡＣ値の検証により、この改竄を検出することができる。したがって、パケット処理装置１０は、ステップＳＴ１の２回目に送信された集約パケットのうち、シーケンス番号３番と５番の個別パケットを破棄する。

シーケンス番号１、２及び６番の個別パケットは、２回送信された集約パケットのいずれにおいても改竄されていないので、パケット処理装置１０に正常に到着している。シーケンス番号３番及び４番の個別パケットは、２回送信された集約パケットのうちの片方のみが改竄されていたので、もう片方については、パケット処理装置１０に正常に到着している。しかしながら、シーケンス番号５番の個別パケットは、２回送信された集約パケットのいずれにおいて改竄されているので、いずれにおいても破棄されている。

【０１３５】

ステップＳＴ２においてパケット処理装置１０は、正常に到着しているシーケンス番号１～４及び６番の個別パケットを、それぞれの宛先であるクライアント装置３０に送信する。なお、図１５に示すクライアント装置３０には、１又は複数のクライアント装置３０が含まれるものとする。

【０１３６】

ステップＳＴ３においてパケット処理装置１０は、シーケンス番号５番の個別パケットを再送するようにサーバー装置２０に要求するため、再送要求をサーバー装置２０に送信する。

【０１３７】

再送要求を受け取ったサーバー装置２０は、シーケンス番号５番の個別パケットを含む集約パケットを生成する。このとき、サーバー集約バッファーには、シーケンス番号７番の個別パケットが登録されているものとする。したがって、サーバー装置２０は、シーケンス番号５番の個別パケットに加えてシーケンス番号７番の個別パケットをも含む集約パケットを生成する。

そして、ステップＳＴ４においてサーバー装置２０は、生成した集約パケットをパケット処理装置１０に送信する。なお、サーバー装置２０は、一例として、生成した当該集約パケットを２回、パケット処理装置１０に送信するものとする。

【０１３８】

パケット処理装置１０は、サーバー装置２０がステップＳＴ４で２回送信した集約パケットを受信する。ここで、ステップＳＴ４の１回目に送信された集約パケットのうち、集約ヘッダーが改竄されていたものとする。パケット処理装置１０は、ＭＡＣ値の検証により、この改竄を検出することができる。したがって、パケット処理装置１０は、ステップＳＴ１の１回目に送信された集約パケットを破棄する。また、ステップＳＴ４の２回目に送信された集約パケットは改竄されていないものとする。したがって、シーケンス番号５番と７番の個別ヘッダーは、パケット処理装置１０に正常に到着している。

【０１３９】

ステップＳＴ５においてパケット処理装置１０は、正常に到着しているシーケンス番号５及び７番の個別パケットを、それぞれの宛先であるクライアント装置３０に送信する。

【０１４０】

第３実施形態の通信システム１によれば、パケット処理装置１０及びサーバー装置２０は、受信した集約パケットに含まれる個別パケットが、改竄されているなどしてデータの完全性の保証が得られなかった場合には、集約パケットのうちの改竄されている個別パケットだけを再送要求する。このため、集約パケットに含まれる個別パケットのうちの一部だけが改竄されている場合には、当該集約パケット全体を再送することが不要である。対し

て、従来では、改竄などが一部に対するものであっても当該集約パケット全体の再送が必要となる。したがって、第３実施形態の通信システム１では、再送されるデータの量が従来よりも少ない。また、再送の頻度も減少するので、従来よりもリアルタイム性が向上する。

【０１４１】

また、第３実施形態の通信システム１によれば、パケット処理装置１０及びサーバー装置２０は、集約パケットを一度に複数回送信する。これにより、集約パケットを受信したパケット処理装置１０又はサーバー装置２０は、一度目に受信した集約パケットに含まれる個別パケットを破棄した場合でも、すぐに次の集約パケットを受信する。したがって、当該パケット処理装置１０又はサーバー装置２０は、再送を要求したことによって再送される個別パケットを受信するよりもすぐに、破棄した個別パケットを受け取ることができる。これにより、リアルタイム性が向上する。

【０１４２】

第１実施形態～第３実施形態は以下のような変形も可能である。

パケット処理装置１０は、ネットワークＮＷ１、ネットワークＮＷ２又はその両方に接続する機能を備えていなくても良い。そして、パケット処理装置１０に接続される装置がネットワークＮＷ１、ネットワークＮＷ２又はその両方に接続して、サーバー装置２０又はクライアント装置３０などと通信を行っても良い。

パケット処理装置１０は、ネットワークＮＷ２を介さずにＵＳＢ（universal serial bus）などのバスによってサーバー装置２０と接続されていても良い。また、サーバー装置２０がパケット処理装置１０を内蔵していても良い。

【０１４３】

プロセッサー１１は、ステップＳ１３において、容量Ｄ１に代えて、集約バッファー１０２に記憶されている未送信の個別パケットの数が予め定められた数以上になったか否かを判定しても良い。また、プロセッサー２１は、ステップＳ１２３において、容量Ｄ２に代えて、サーバー集約バッファーに記憶されている未送信の個別パケットの数が予め定められた数以上になったか否かを判定しても良い。上記の態様は、個別パケットのデータサイズがほとんど一定であるような場合などに用いることができる。

【０１４４】

プロセッサー１１又はプロセッサー２１は、集約するパケットを全て集約バッファー１０２又はサーバー集約バッファーから取り出し、その後に集約を行っても良い。

【０１４５】

パケット処理装置１０又はサーバー装置２０は、送信する個別パケットが１個のみ場合には集約パケットの形にせずにそのまま送信しても良い。

【０１４６】

第１実施形態の通信システム１は、破棄したパケットの再送を要求しない態様であっても良い。すなわち、プロセッサー１１は、ステップＳ３８をスキップしてステップＳ３１へと進む。また、プロセッサー２１は、ステップＳ１０８をスキップしてステップＳ１０１へと進む。

【０１４７】

第１実施形態～第３実施形態では、サーバー装置２０が１台である例について示した。しかしながら、複数のサーバー装置２０がネットワークＮＷに接続されていても良い。この場合、パケット処理装置１０は、受信した個別パケットを、例えば、宛先となるサーバー装置２０が同じものだけを対象として集約を行う。すなわち、パケット処理装置１０は、宛先別に集約パケットを生成及び送信する。

【０１４８】

複数のパケット処理装置１０を用いて、例えば、２地点間の通信を効率化することができる。例えば、第１のパケット処理装置１０及び第１のパケット処理装置１０と通信可能な複数の装置（以下「装置ａ」という。）がＡ地点に、第２のパケット処理装置１０及び第２のパケット処理装置１０と通信可能な複数の装置（以下「装置ｂ」という。）がＢ地点

に設置されているとする。この場合、第１のパケット処理装置１０は、複数の装置ａから送信された、装置ｂを宛先とする個別パケットを集約した集約パケットを第２のパケット処理装置１０に送信する。そして、第２のパケット処理装置１０は、受信した当該集約パケットを個々の個別パケットに分割し、それぞれの個別パケットをそれぞれの宛先である装置ｂに送信する。また、第２のパケット処理装置１０は、複数の装置ｂから送信された、装置ａを宛先とする個別パケットを集約した集約パケットを第１のパケット処理装置１０に送信する。そして、第１のパケット処理装置１０は、受信した当該集約パケットを個々の個別パケットに分割し、それぞれの個別パケットをそれぞれの宛先である装置ａに送信する。

【０１４９】

第１実施形態～第３実施形態に示す通信システム１は、サーバークライアントモデルであるが、サーバークライアントモデルには限らない。

【０１５０】

通信システム１は、ＭＡＣ以外を用いてデータの完全性の保証及び検証を行っても良い。例えば、通信システム１は、ＭＩＣ（message integrity code）を用いる。ＭＩＣは、データの完全性を保証するための符号の一例である。

【０１５１】

パケット処理装置１０及びサーバー装置２０は、集約パケットに誤り訂正符号を付与しても良い。

【０１５２】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

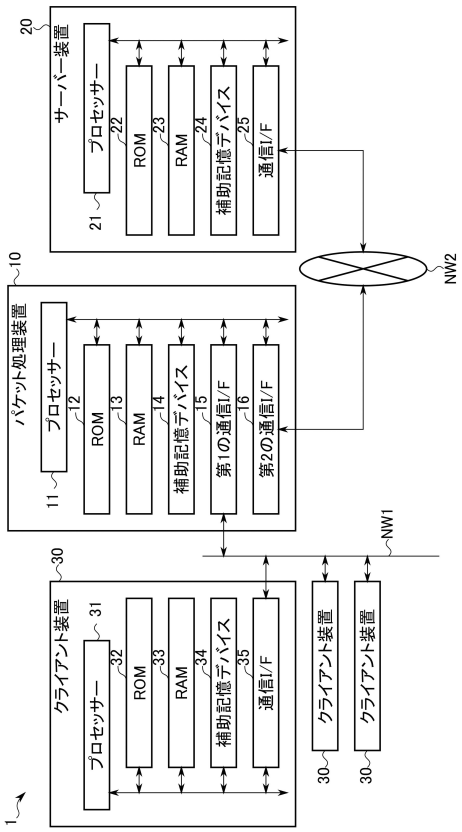
【符号の説明】

【０１５３】

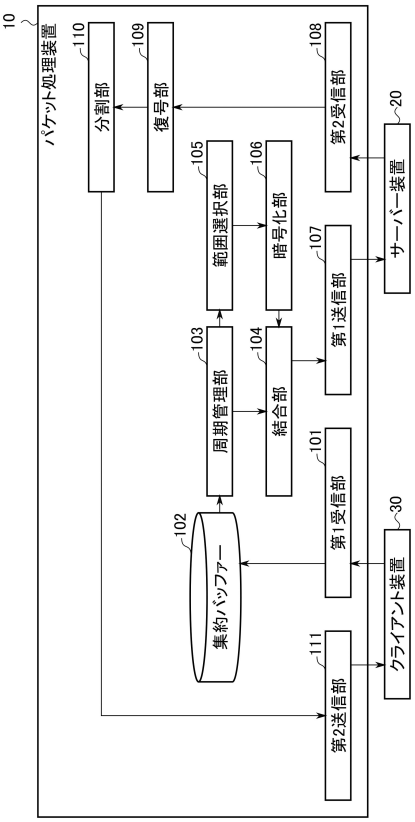
１……通信システム、１０……パケット集約装置、１１，２１，３１……プロセッサー、１２，２２，３２……ＲＯＭ、１３，２３，３３……ＲＡＭ、１４，２４，３４……補助記憶デバイス、１５……第１の通信Ｉ／Ｆ、１６……第２の通信Ｉ／Ｆ、２０……サーバー装置、２５，３５……通信Ｉ／Ｆ、３０……クライアント装置、１０１……第１受信部、１０２……集約バッファー、１０３……周期管理部、１０４……結合部、１０５……範囲選択部、１０６，１２４……暗号化部、１０７……第１送信部、１０８……第２受信部、１０９，１２５……復号部、１１０……分割部、１１１……第２送信部、１２１……冗長化部、１２２……再送要求部、１２３……到着管理部

【図面】

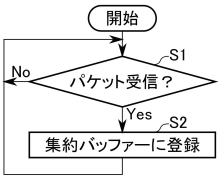
【図１】


サーバー装置
プロセッサー
ROM
RAM
補助記憶デバイス
通信I/F
パケット処理装置
第1の通信I/F
第2の通信I/F
クライアント装置
NW1
NW2

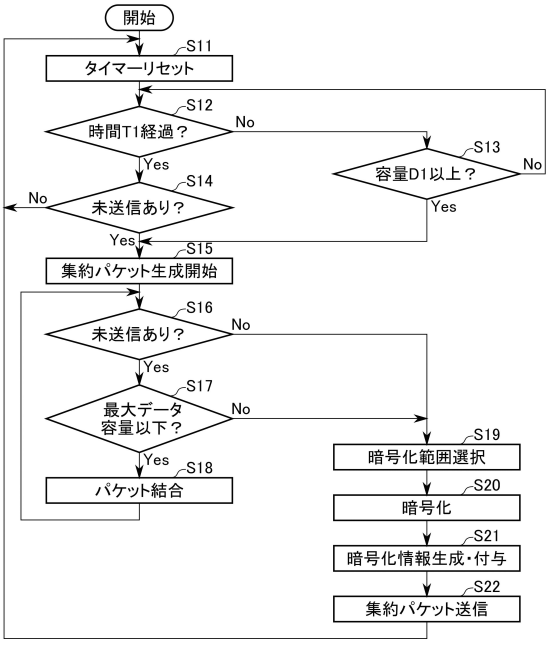
【図２】


パケット処理装置
分割部
復号部
第2受信部
サーバー装置
範囲選択部
暗号化部
第1送信部
周期管理部
結合部
第1受信部
集約バッファー
クライアント装置
第2送信部

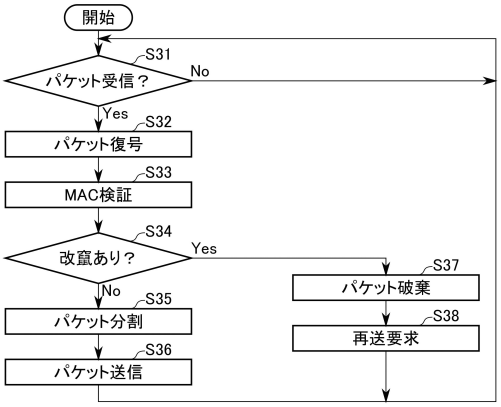
【図３】


開始
パケット受信？
No
Yes
集約バッファーに登録

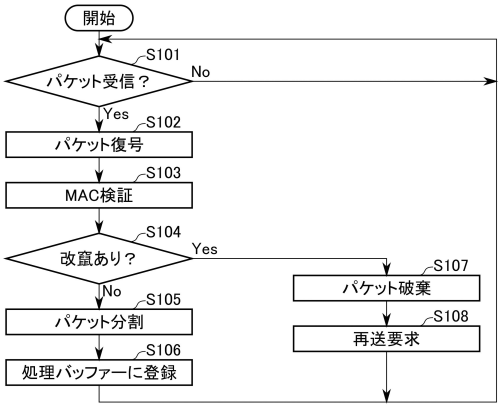
【図４】


開始
タイマーリセット
時間T1経過？
No
Yes
容量D1以上？
No
Yes
未送信あり？
No
Yes
集約パケット生成開始
未送信あり？
No
Yes
最大データ容量以下？
No
Yes
パケット結合
暗号化範囲選択
暗号化
暗号化情報生成・付与
集約パケット送信

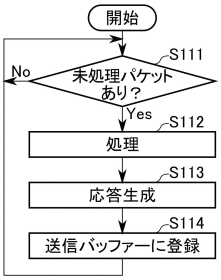
【図５】


開始
S31
パケット受信？
No
Yes
S32
パケット復号
S33
MAC検証
S34
改竄あり？
Yes
No
S35
パケット分割
S36
パケット送信
S37
パケット破棄
S38
再送要求

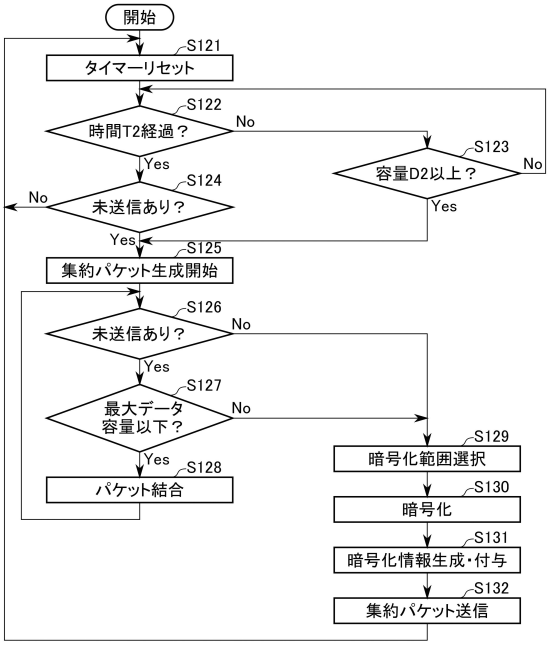
【図６】


開始
S101
パケット受信？
No
Yes
S102
パケット復号
S103
MAC検証
S104
改竄あり？
Yes
No
S105
パケット分割
S106
処理バッファーに登録
S107
パケット破棄
S108
再送要求

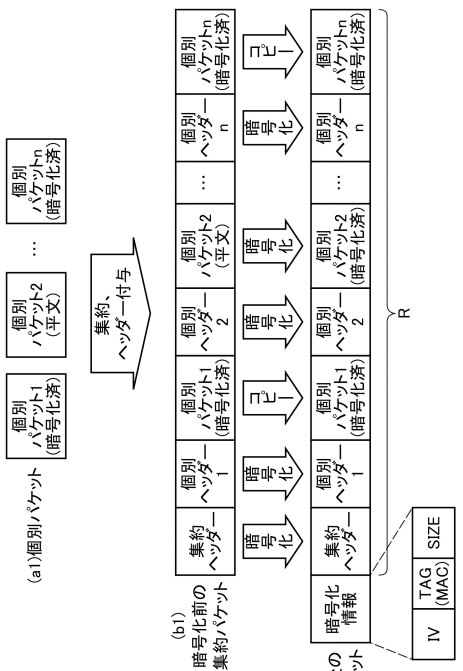
【図７】


開始
S111
未処理パケット
あり？
No
Yes
S112
処理
S113
応答生成
S114
送信バッファーに登録

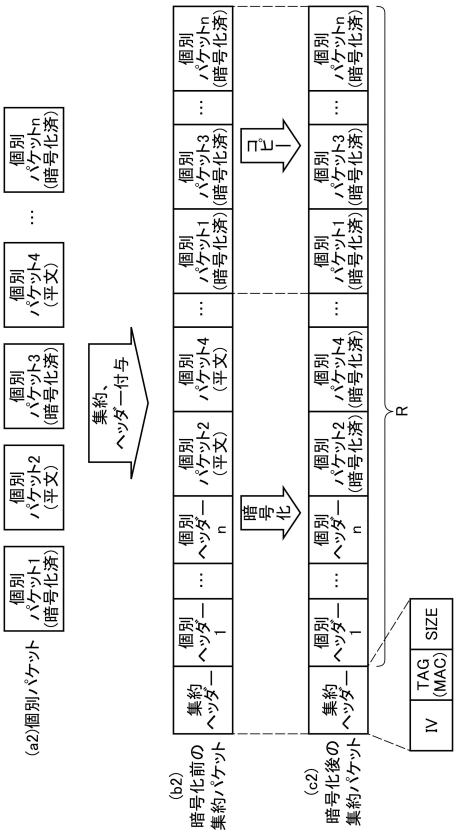
【図８】


開始
S121
タイマーリセット
S122
時間T2経過？
No
Yes
S123
容量D2以上？
No
Yes
S124
未送信あり？
No
Yes
S125
集約パケット生成開始
S126
未送信あり？
No
Yes
S127
最大データ
容量以下？
No
Yes
S128
パケット結合
S129
暗号化範囲選択
S130
暗号化
S131
暗号化情報生成・付与
S132
集約パケット送信

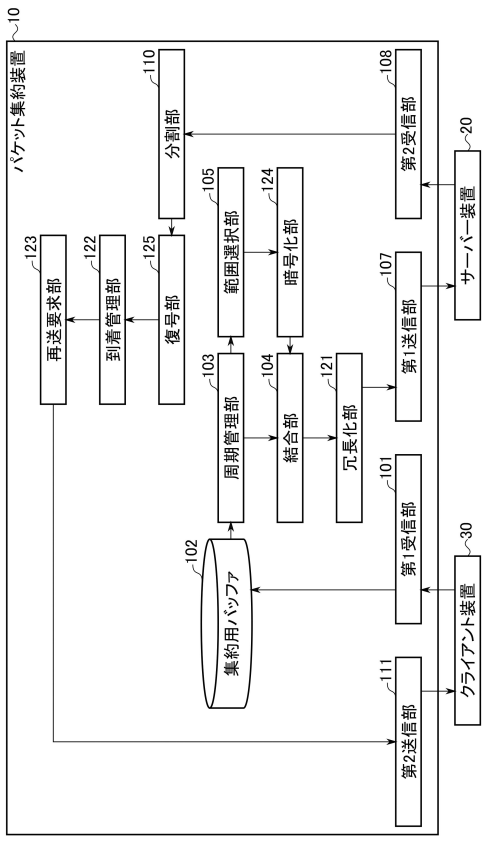
【図９】



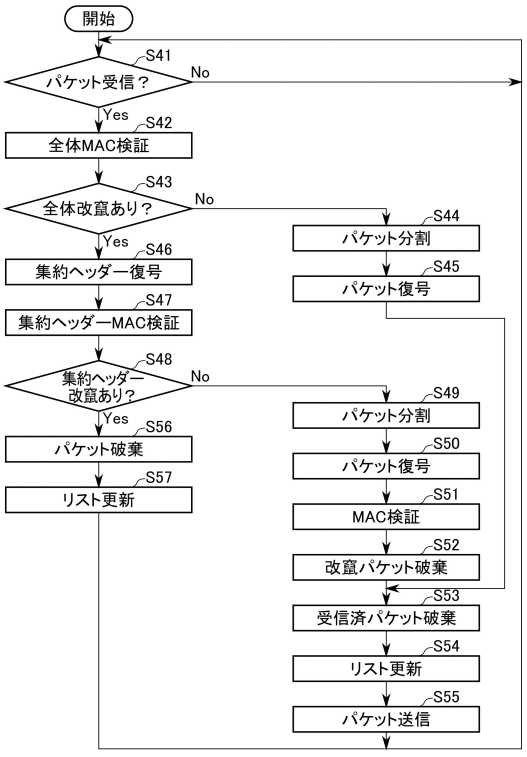
【図１０】



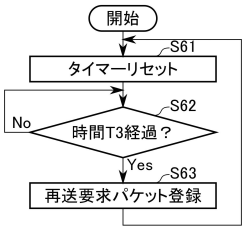
【図１１】



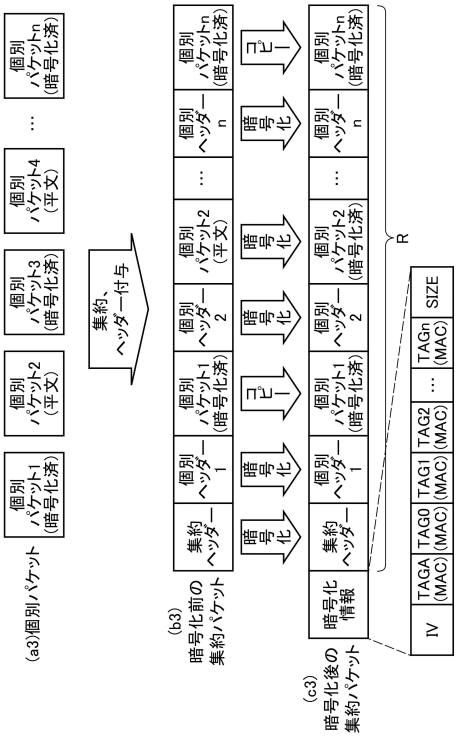
【図１２】



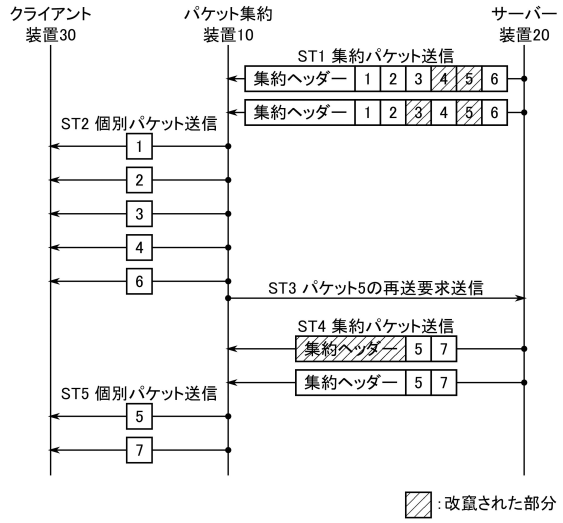
【図１３】


開始
S61
タイマーリセット
S62
No
時間T3経過？
Yes
S63
再送要求パケット登録

【図１４】


個別パケット1（暗号化済）
個別パケット2（平文）
個別パケット3（暗号化済）
個別パケット4（平文）
…
個別パケットn（暗号化済）
(a3)個別パケット
集約、ヘッダー付与
集約ヘッダー
個別ヘッダー1
個別パケット1（暗号化済）
個別ヘッダー2
個別パケット2（平文）
…
個別ヘッダーn
個別パケットn（暗号化済）
(b3)暗号化前の集約パケット
暗号化
コピー
暗号化情報
IV
TAGA（MAC）
TAG0（MAC）
TAG1（MAC）
TAG2（MAC）
…
TAGn（MAC）
SIZE
R
(c3)暗号化後の集約パケット

【図１５】


クライアント装置30
パケット集約装置10
サーバー装置20
ST1 集約パケット送信
集約ヘッダー 1 2 3 4 5 6
集約ヘッダー 1 2 3 4 5 6
ST2 個別パケット送信
1
2
3
4
6
ST3 パケット5の再送要求送信
ST4 集約パケット送信
集約ヘッダー 5 7
集約ヘッダー 5 7
ST5 個別パケット送信
5
7
：改竄された部分

フロントページの続き

鵜飼 健
(72)発明者 金井 遵
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 大西 直哉
東京都港区芝浦一丁目１番１号 株式会社東芝内
(72)発明者 松山 拓紀
東京都港区芝浦一丁目１番１号 株式会社東芝内
審査官 中川 幸洋
(56)参考文献 特開２００７－０３６８３４（ＪＰ，Ａ）
特開２００３－１６９０９２（ＪＰ，Ａ）
特開２０１４－０３９１１１（ＪＰ，Ａ）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／９５１