(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5205075号
(P5205075)
(45)発行日　平成25年6月5日(2013.6.5)　(24)登録日　平成25年2月22日(2013.2.22)

(51)Int.Cl.　F I
H04L 9/36 (2006.01)　H04L 9/00 685
H04L 12/22 (2006.01)　H04L 12/22

請求項の数 4　(全 20 頁)

(21)出願番号　特願2008-32228(P2008-32228)
(22)出願日　平成20年2月13日(2008.2.13)
(65)公開番号　特開2009-194559(P2009-194559A)
(43)公開日　平成21年8月27日(2009.8.27)
審査請求日　平成22年9月13日(2010.9.13)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100105050
弁理士　鷲田　公一
(72)発明者　山田　一成
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　千賀　諭
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　リュウ　シュエ　タン
台湾１０６５７台北市大安区仁愛路３段１３６号１０楼１００２室　パナソニック台湾研究所内

最終頁に続く

(54)【発明の名称】暗号処理方法、暗号処理装置、復号処理方法および復号処理装置

(57)【特許請求の範囲】
【請求項１】
セキュリティプロトコルによってセキュア化されたマルチメディア通信に対する暗復号処理または認証処理を増進するための暗号処理装置における暗号処理方法であり、
前記マルチメディア通信の開始時に、暗復号処理または認証処理が必要なパケットを識別するための識別条件を含むセキュア処理情報を記憶装置またはメモリに記憶するステップと、
平文のマルチメディアパケットを仮想ネットワークインタフェースへ送信するステップと、
前記セキュア処理情報に含まれる前記識別条件に基づいて前記平文のマルチメディアパケットをネットワークプロトコルスタック内でフィルタリングするステップと、
前記平文のマルチメディアパケットがフィルタリングされるときに、前記平文のマルチメディアパケットが前記セキュア処理情報に含まれる前記識別条件と合致する場合、前記平文のマルチメディアパケットに対して暗号処理または認証処理を実行して、セキュリティプロトコルに適合するように、セキュアマルチメディアパケットのペイロードを修正するステップと、
前記仮想ネットワークインタフェースへの宛先アドレスを、前記セキュアマルチメディアパケットの送信先アドレスに置き換えるステップと、
前記セキュアマルチメディアパケットをネットワークインタフェースから送出するステップと、

を有する暗号処理方法。
【請求項２】
セキュリティプロトコルによってセキュアされたマルチメディア通信に対する暗復号処理または認証処理を増進するための暗号処理装置であり、
暗復号処理または認証処理が必要なパケットを識別するための識別条件を含むセキュア処理情報を記憶する記憶手段と、
平文のマルチメディアパケットを仮想ネットワークインタフェースへ送信する送信手段と、
前記平文のマルチメディアパケットが前記セキュア処理情報に含まれる前記識別条件と合致するか否かを判断し、前記識別条件が合致した場合に前記平文のマルチメディアパケットに対して暗号処理または認証処理を実行して、セキュリティプロトコルに適合するようにセキュアマルチメディアパケットのペイロードを修正する修正手段と、
前記仮想ネットワークインタフェースへの宛先アドレスを、前記セキュアマルチメディアパケットの送信先アドレスに置き換える置換手段と、
前記セキュアマルチメディアパケットをネットワークインタフェースから送出する送出手段と、
を有する暗号処理装置。
【請求項３】
セキュリティプロトコルによってセキュアされたマルチメディア通信に対する暗復号処理または認証処理を増進するための復号処理装置における復号処理方法であり、
前記マルチメディア通信の開始時に、暗復号処理または認証処理が必要なパケットを識別するための識別条件を含むセキュア処理情報を記憶装置またはメモリに記憶するステップと、
前記セキュア処理情報に含まれる前記識別条件に基づいて、入力されるセキュアマルチメディアパケットをネットワークプロトコルスタック内でフィルタリングするステップと、
前記セキュアマルチメディアパケットがフィルタリングされるときに、前記セキュアマルチメディアパケットが前記セキュア処理情報に含まれる前記識別条件と合致する場合、前記セキュアマルチメディアパケットに対して復号処理または認証処理を実行し、前記セキュアマルチメディアパケットのペイロードを平文ペイロードとして修正するステップと、
平文のマルチメディアパケットを入力マルチメディア通信のアプリケーション層へ送信するステップと、
を有する復号処理方法。
【請求項４】
セキュリティプロトコルによってセキュアされた入力マルチメディア通信に対する暗復号処理または認証処理を増進するための復号処理装置であり、
暗復号処理または認証処理が必要なパケットを識別するための識別条件を含むセキュア処理情報を記憶するための記憶手段と、
入力されるセキュアマルチメディアパケットが前記セキュア処理情報に含まれる前記識別条件と合致するか否かを判断し、前記識別条件が合致する場合に前記セキュアマルチメディアパケットに対して復号処理または認証処理を実行し、セキュアマルチメディアパケットのペイロードを平文ペイロードとして修正するための修正手段と、
平文のマルチメディアパケットを入力マルチメディア通信のアプリケーション層へ送信する送信手段と、
を有する復号処理装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、アプリケーション層のセキュリティを増進するための暗号処理方法、暗号処

理装置、復号処理方法および復号処理装置に関する。
【背景技術】
【０００２】
特許文献１は、アプリケーション層セキュリティプロトコルに対応した処理性能を増進する方法を提案している。特許文献１は、処理性能を増進するために、暗号化アクセラレータが暗号処理の負荷をＣＰＵから取り除くことを開示する。しかし、特許文献１に開示された方法では、各入力メッセージまたは出力メッセージごとにユーザ空間とカーネル空間の間で２回のメモリコピー動作が発生し、大きなオーバヘッドを招く。
【０００３】
そこで、アプリケーション層セキュリティプロトコルにおけるユーザ-カーネル空間でのメモリコピーのオーバヘッドに対処するために、次の発明が提案されている（特許文献２）。
【０００４】
特許文献２は、暗号処理とネットワークプロトコルスタック処理の両方の負荷を暗号化アクセラレータと、ネットワークプロトコルスタックプロセッサとの両方からなるネットワークプロトコルオフロードチップに担わせることにより、メモリコピーのオーバヘッドを減少させる方法を提案している。しかし、この方法を実現するには特定のネットワークハードウェア構成が必要であり、装置に組み込まれたソフトウェアベースのＴＣＰ／ＩＰスタックには適合しない。
【特許文献１】米国特許第７，０４７，４０５号明細書
【特許文献２】米国特許第６，９８３，３８２号明細書
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、特許文献１では、アプリケーション層セキュリティプロトコルを実行するとき、各入力メッセージまたは出力メッセージごとに、ユーザ空間とカーネル空間との間で、各マルチメディアペイロードを複数回のメモリコピーを行うため、暗号処理性能が悪いという問題が生じる。ここで、ペイロードとはデータブロックのうちヘッダ等をのぞいたデータ本体を指す。オーディオビデオ等の大きいサイズのペイロードを処理する際には、この性能はより悪化する。
【０００６】
特許文献２では、メモリコピーのオーバヘッドを回避できても、大きいサイズのペイロードのセグメント化された部分の連続を処理する場合、連続する二つのセグメントを関係付けるための暗号化に関する情報がないので、アプリケーション層セキュアプロトコルを適用する際、各セグメントに対して個々にＣＢＣまたはカウンターモードの暗号化および認証処理を行う際に困難が生じる。
【０００７】
本発明は、かかる点に鑑みてなされたものであり、セキュアマルチメディア通信の暗復号処理性能または認証処理性能を効果的に増進する暗号処理方法、暗号処理装置、復号処理方法および復号処理装置を提供することを目的とする。
【課題を解決するための手段】
【０００８】
本発明の暗号処理方法は、セキュリティプロトコルによってセキュア化されたマルチメディア通信に対する暗復号処理または認証処理を増進するための暗号処理装置における暗号処理方法であり、前記マルチメディア通信の開始時に、暗復号処理または認証処理が必要なパケットを識別するための識別条件を含むセキュア処理情報を記憶装置またはメモリに記憶するステップと、平文のマルチメディアパケットを仮想ネットワークインタフェースへ送信するステップと、前記セキュア処理情報に含まれる前記識別条件に基づいて前記平文のマルチメディアパケットをネットワークプロトコルスタック内でフィルタリングするステップと、前記平文のマルチメディアパケットがフィルタリングされるときに、前記

平文のマルチメディアパケットが前記セキュア処理情報に含まれる前記識別条件と合致する場合、前記平文のマルチメディアパケットに対して暗号処理または認証処理を実行して、セキュリティプロトコルに適合するように、セキュアマルチメディアパケットのペイロードを修正するステップと、前記仮想ネットワークインタフェースへの宛先アドレスを、前記セキュアマルチメディアパケットの送信先アドレスに置き換えるステップと、前記セキュアマルチメディアパケットをネットワークインタフェースから送出するステップと、を有するようにした。

【０００９】

本発明の暗号処理装置は、セキュリティプロトコルによってセキュアされたマルチメディア通信に対する暗復号処理または認証処理を増進するための暗号処理装置であり、暗復号処理または認証処理が必要なパケットを識別するための識別条件を含むセキュア処理情報を記憶する記憶手段と、平文のマルチメディアパケットを仮想ネットワークインタフェースへ送信する送信手段と、前記平文のマルチメディアパケットが前記セキュア処理情報に含まれる前記識別条件と合致するか否かを判断し、前記識別条件が合致した場合に前記平文のマルチメディアパケットに対して暗号処理または認証処理を実行して、セキュリティプロトコルに適合するようにセキュアマルチメディアパケットのペイロードを修正する修正手段と、前記仮想ネットワークインタフェースへの宛先アドレスを、前記セキュアマルチメディアパケットの送信先アドレスに置き換える置換手段と、前記セキュアマルチメディアパケットをネットワークインタフェースから送出する送出手段と、を有する構成を採る。

【００１０】

本発明の復号処理方法は、セキュリティプロトコルによってセキュアされたマルチメディア通信に対する暗復号処理または認証処理を増進するための復号処理装置における復号処理方法であり、前記マルチメディア通信の開始時に、暗復号処理または認証処理が必要なパケットを識別するための識別条件を含むセキュア処理情報を記憶装置またはメモリに記憶するステップと、前記セキュア処理情報に含まれる前記識別条件に基づいて、入力されるセキュアマルチメディアパケットをネットワークプロトコルスタック内でフィルタリングするステップと、前記セキュアマルチメディアパケットがフィルタリングされるときに、前記セキュアマルチメディアパケットが前記セキュア処理情報に含まれる前記識別条件と合致する場合、前記セキュアマルチメディアパケットに対して復号処理または認証処理を実行し、セキュアマルチメディアパケットのペイロードを平文ペイロードとして修正するステップと、平文のマルチメディアパケットを入力マルチメディア通信のアプリケーション層へ送信するステップと、を有するようにした。

【００１１】

本発明の復号処理装置は、セキュリティプロトコルによってセキュアされた入力マルチメディア通信に対する暗復号処理または認証処理を増進するための復号処理装置であり、暗復号処理または認証処理が必要なパケットを識別するための識別条件を含むセキュア処理情報を記憶するための記憶手段と、入力されるセキュアマルチメディアパケットが前記セキュア処理情報に含まれる前記識別条件と合致するか否かを判断し、前記識別条件が合致する場合に前記セキュアマルチメディアパケットに対して復号処理または認証処理を実行し、前記セキュアマルチメディアパケットのペイロードを平文ペイロードとして修正するための修正手段と、平文のマルチメディアパケットを入力マルチメディア通信のアプリケーション層へ送信する送信手段と、を有する構成を採る。

【発明の効果】

【００１２】

本発明によれは、セキュアマルチメディア通信の暗復号処理性能または認証処理性能を効果的に増進することができる。

【発明を実施するための最良の形態】

【００１３】

以下、本発明の実施の形態について、図面を参照して詳細に説明する。

【００１４】
本実施の形態では、大きいサイズのペイロードを、ネットワークへ実際に送出する際に使用される最大送信単位よりも十分に大きい最大送信単位を設定した仮想ネットワーク装置（仮想ネットワークインタフェース）に転送し、仮想ネットワーク装置のネットワークプロトコルスタックにいったん取り込んだ大きいサイズのペイロード全体に対して、カーネルレベルの暗復号処理または認証処理を起動し、セキュア化されたペイロードを実在のネットワーク装置（ネットワークインタフェース）のネットワークプロトコルスタックに送信する構成について説明する。
【００１５】
図１は、本発明の実施の形態に係る暗号処理通信システムの一例を示す構成図である。
【００１６】
暗号処理通信システム１００は、ユーザ空間１１０とカーネル空間１２０を含む。
【００１７】
ユーザ空間１１０は、セキュアマルチメディアアプリケーション１１２、ソケット１１４、セキュアマルチメディアアプリケーションの統制部１１６、およびセキュア制御インタフェース１１８を含む。
【００１８】
セキュアマルチメディアアプリケーション１１２は、セキュアリアルタイムトランスポートプロトコル（ＳＲＴＰ）等のアプリケーション層セキュリティプロトコルの保護の下で、インターネットを介してオーディオまたはビデオ等のマルチメディアコンテンツを楽しむアプリケーションである。
【００１９】
オーディオまたはビデオ等のマルチメディアコンテンツは、ペイロードの形でパケット化される。高精細度のマルチメディアコンテンツがトレンドであるので、ペイロードは、一般に、大きいサイズのペイロードになる。
【００２０】
マルチメディアコンテンツを運ぶペイロードは、ネットワーク処理のためにソケット１１４に入力される。
【００２１】
セキュアマルチメディアアプリケーション１１２は、セキュアマルチメディアアプリケーションの統制部１１６によって、セキュアマルチメディア通信を起動する。
【００２２】
セキュアマルチメディアアプリケーションの統制部１１６は、セキュアマルチメディア通信の開始や終了等のコマンドをセキュア制御インタフェース１１８へ送る。
【００２３】
カーネル空間１２０は、ネットワークプロトコルスタック１３０、仮想ネットワークインタフェース１４０、ネットワークインタフェース１５０、およびカーネルレベル暗号モジュール１６０から構成される。
【００２４】
ネットワークプロトコルスタック１３０は、セキュアマルチメディアパケットの出力フィルタ１３２、およびセキュアマルチメディアパケットの入力フィルタ１３４から構成される。
【００２５】
ネットワークプロトコルスタック１３０の一例としては、ＴＣＰ／ＩＰスタックがある。
【００２６】
仮想ネットワークインタフェース１４０としては、大きいサイズのマルチメディアペイロードをセグメントに分割するのを避けるために比較的大きなＭＴＵ（最大送信単位）をもつ仮想ネットワークインタフェースを設定する。
【００２７】

セキュアマルチメディアアプリケーションの統制部１１６は、セキュアマルチメディアパケットの出力フィルタ１３２と、セキュアマルチメディアパケットの入力フィルタ１３４とを設定および起動する。

【００２８】

マルチメディアパケットが、出力フィルタ１３２、または、入力フィルタ１３４でフィルタリングされるとき、マルチメディアパケットが出力フィルタ１３２、または、入力フィルタ１３４にて設定された識別条件を満たせば、マルチメディアパケットのペイロードはアプリケーション層セキュリティプロトコルに適合する暗復号処理または認証処理を受ける。ここで、識別条件は、暗復号処理または認証処理に必要なパラメタであり、または暗復号処理または認証処理が必要なパケットを識別するための条件である。

【００２９】

カーネルレベル暗号モジュール１６０は、アプリケーション層セキュア処理情報格納部１６２、アプリケーション層セキュリティ処理ユニット１６４、および暗号処理ユニット１６８から構成される。なお、暗号処理ユニット１６８は、暗号ユニット１６８２とメッセージ認証ユニット１６８４を含む。カーネルレベル暗号モジュール１６０は、アプリケーション層セキュリティプロトコルに適合する暗号処理または認証処理を実行する。

【００３０】

図２は、出力されるセキュアマルチメディアパケットに対してカーネルレベル暗号処理または認証処理を実行するための本発明の実施の形態を示すフローチャートである。

【００３１】

ステップＳ１０２において、セキュアマルチメディアアプリケーション１１２は、セキュアマルチメディアアプリケーション自身の処理を開始し、出力セキュアマルチメディアパケットに対応した設定を行うように、セキュアマルチメディアアプリケーションの統制部１１６を起動する。

【００３２】

これにより、セキュアマルチメディアアプリケーションの統制部１１６は、仮想ネットワークインタフェース１４０のネットワークプロトコルスタック１３０内で、一つの出力暗号処理フィルタリングポイント１３２を有効化する。そして、統制部１１６は、アプリケーション層セキュア処理情報格納部１６２（本発明の「記憶手段」に相当）中にセキュア処理情報エントリーを作成し、アプリケーション層セキュリティ処理ユニット１６４および暗号処理ユニット１６８における暗号処理または認証処理の設定を含む、カーネルレベル暗号モジュール１６０の設定を行う。

【００３３】

ステップＳ１０４において、ユーザ空間１１０で出力マルチメディアコンテンツが発生すると、セキュアマルチメディアアプリケーション１１２は、マルチメディアトランスポートパケットを生成する。

【００３４】

ステップＳ１０６において、セキュアマルチメディアアプリケーション１１２は、マルチメディアトランスポートパケットを、ソケット１１４を介して、仮想ネットワークインタフェース１４０のネットワークプロトコルスタック１３０へ送信する。

【００３５】

ステップＳ１０８で、カーネル空間１２０において、マルチメディアトランスポートパケットが出力フィルタ１３２の識別条件を満たす場合は、ネットワークプロトコルスタック１３０は、カーネルレベル暗号モジュール１６０を起動して、マルチメディアトランスポートパケットに対する暗号処理または認証処理を行わせ、アプリケーション層セキュリティに適合するようにペイロードを修正させる。

【００３６】

アプリケーション層セキュア処理情報格納部１６２中のセキュア処理情報エントリーに基づいて、カーネルレベル暗号モジュール１６０は、暗号ユニット１６８２において、マルチメディアトランスポートパケットの暗号化を実行する。メッセージ認証ユニット１６

８４は、メッセージ認証を実行する。そして、アプリケーション層セキュリティ処理ユニット１６４は、例えば、ＳＲＴＰにより暗号化された部分と、ＳＲＴＰにより認証された部分とに適合するような、アプリケーション層セキュリティをもつペイロードにマルチメディアトランスポートパケットを作り変える。すなわち、マルチメディアトランスポートパケットは、セキュアマルチメディアパケットに変換される。

【００３７】

ステップＳ１１０において、アプリケーション層セキュリティ処理ユニット１６４は、仮想ネットワークインタフェースになっているセキュアマルチメディアパケットの宛先アドレスを実際の送信先である送信先アドレスに置き換える。

【００３８】

ステップＳ１１２において、セキュアマルチメディアパケットはネットワークインタフェース１５０のネットワークプロトコルスタック１３０へ送信される。

【００３９】

ステップＳ１１４で、ネットワークインタフェース１５０のネットワークプロトコルスタック１３０において、セキュアマルチメディアパケットは、ペイロードサイズをネットワークインタフェース１５０のＭＴＵに照らし合わせて、パケットのセグメント分割を行うか否かが判断される。セグメント分割条件に合う場合は、ステップＳ１１６へ進み、パケット分割を行い、生成された複数の分割されたパケットをネットワークインタフェース１５０から送出する。そうでない場合は、ステップＳ１１８へ進み、セキュアマルチメディアパケットをネットワークインタフェース１５０から送出する。

【００４０】

図３は、入力されるセキュアマルチメディアパケットに対してカーネルレベル復号処理または認証処理を実行するための本発明の実施の形態を示すフローチャートである。

【００４１】

ステップＳ２０２において、セキュアマルチメディアアプリケーション１１２が、セキュアマルチメディアアプリケーションを始動し、入力されるセキュアマルチメディアアプリケーションに対応した設定を行うように、セキュアマルチメディアアプリケーションの統制部１１６を起動する。

【００４２】

これにより、セキュアマルチメディアアプリケーションの統制部１１６は、ネットワークインタフェース１５０のネットワークプロトコルスタック１３０内で、一つの入力暗号処理フィルタリングポイント１３４を有効化する。そして統制部１１６は、アプリケーション層セキュア処理情報格納部１６２（本発明の「記憶手段」に相当）中にセキュア処理情報エントリーを作成し、アプリケーション層セキュリティ処理ユニット１６４および暗号処理ユニット１６８における復号処理または認証処理の設定を含む、カーネルレベル暗号モジュール１６０の設定を行う。

【００４３】

ステップＳ２０４で、入力されるセキュアマルチメディアパケットがネットワークインタフェース１５０により受信され、その後のネットワークプロトコル処理のためにスケジュールされる。

【００４４】

ステップＳ２０６において、カーネル空間１２０において、マルチメディアパケットが、入力フィルタ１３４の識別条件を満たす場合は、ネットワークプロトコルスタック１３０は、カーネルレベル暗号モジュール１６０を起動して、パケットの復号処理または認証処理を行わせ、ペイロードがアプリケーション層セキュリティに適合することを確認させる。

【００４５】

アプリケーション層セキュア処理情報格納部１６２中のセキュア処理情報エントリーに基づいて、カーネルレベル暗号モジュール１６０は、暗号ユニット１６８２においてマルチメディアパケットの復号化を実行する。メッセージ認証ユニット１６８４は、セキュア

マルチメディアパケットからメッセージ認証値を算出し、算出結果とセキュアマルチメディアパケットに含まれているメッセージ認証値を照合することにより、セキュリティパケットの信頼性を確認する。これらが厳密に一致する場合、セキュアマルチメディアパケットは本当に信頼できるものであり、通信相手によって真正に送信されていることを意味する。セキュアマルチメディアパケット中のペイロードは、平文のペイロードになる。

【００４６】

ここで、平文とは暗号化する前、または、復号化した後の、暗号化されていない状態のデータを指す。

【００４７】

ステップＳ２０８において、ネットワークプロトコルスタック１３０は、平文のマルチメディアパケットを、ソケット１１４を介してセキュアマルチメディアアプリケーション１１２へ送信する。これにより、セキュアマルチメディアアプリケーション１１２は、平文のマルチメディアパケットを受信する。

【００４８】

図４は、セキュアマルチメディアアプリケーションの統制部、アプリケーション層セキュア処理情報、アプリケーション層セキュリティ処理ユニット、および暗号処理ユニットの構成図である。

【００４９】

セキュアマルチメディアアプリケーションの統制部１１６は、セキュアアプリケーションセッションの開始ユニット１１６２とセキュアアプリケーションセッションの終了ユニット１１６４を含む。

【００５０】

セキュアマルチメディアアプリケーション１１２から出力セキュアマルチメディアアプリケーション開始を受信すると、セキュアアプリケーションセッションの開始ユニット１１６２は、仮想ネットワークインタフェース１４０のネットワークプロトコルスタック１３０内のセキュアマルチメディアパケットの出力フィルタ１３２を起動し、アプリケーション層セキュア処理情報格納部１６２中のエントリーを初期化する。

【００５１】

本実施の形態では、仮想ネットワークインタフェース１４０として、ローカルループバックインタフェースが適用可能であり、フィルタリング方法は、ネットフィルタであり、出力フィルタリングポイント１３２はネットフィルタのＮＦ_ＩＰ_ＬＯＣＡＬ_ＯＵＴである。

【００５２】

セキュアマルチメディアアプリケーション１１２から入力セキュアマルチメディアアプリケーション開始を受信すると、セキュアアプリケーションセッションの開始ユニット１１６２は、ネットワークインタフェース１５０のネットワークプロトコルスタック１３０内のセキュアマルチメディアパケットの入力フィルタ１３４を起動し、アプリケーション層セキュア処理情報格納部１６２中のエントリーを初期化する。

【００５３】

本実施の形態では、仮想ネットワークインタフェース１４０として、イーサネットネット（登録商標）ワークカードが適用可能であり、フィルタリング方法はネットフィルタであり、入力フィルタリングポイント１３４はネットフィルタのＮＦ_ＩＰ_ＬＯＣＡＬ_ＩＮである。

【００５４】

セキュアマルチメディアアプリケーション１１２から入力セキュアまたは出力マルチメディアアプリケーション終了を受信すると、セキュアアプリケーションセッションの終了ユニット１１６４は、ネットフィルタの入力または出力フィルタポイントを無効化することによって、セキュアマルチメディアパケットの入力フィルタ１３４またはセキュアマルチメディアパケットの出力フィルタ１３２を無効化する。

【００５５】

アプリケーション層セキュア処理情報格納部１６２は、複数のセキュア処理情報のエントリーを記憶する。セキュア処理情報の一つのエントリー１６２０は、入力セキュアまたは出力マルチメディアアプリケーションのいずれかに対応する。アプリケーション層セキュア処理情報格納部１６２中のセキュア処理情報の各エントリーは、セキュアマルチメディアアプリケーションを特定するため並びに暗号処理を実行するために必要な暗号化に関する情報を記憶するための複数のフィールドを含む。

【００５６】

セキュア処理情報の一つのエントリー１６２０は、同期ソース（ＳＳＲＣ）識別子１６２１、送信先ネットワークアドレス１６２２、送信先トランスポートポート番号１６２３、暗号アルゴリズム識別子１６２４、認証アルゴリズム識別子１６２５、マスターキー１６２６、マスターＳａｌｔ１６２７、暗号キー１６２８、および認証キー１６２９のフィールドを含む。

【００５７】

ＳＳＲＣ識別子１６２１、送信先ネットワークアドレス１６２２および送信先トランスポートポート番号１６２３は、セキュアアプリケーションの暗号コンテクスト（cryptographic context）を照合するために使用される。

【００５８】

暗号アルゴリズム識別子１６２４は、セキュアアプリケーションの暗号アルゴリズムを特定するために使用される。サポートされるアルゴリズムは、ＣＢＣまたはカウンターモードを含むＤＥＳ、３ＤＥＳ、ＡＥＳ、ＡＥＳ１９２、およびＡＥＳ２５６などである。

【００５９】

認証アルゴリズム識別子１６２５は、セキュアアプリケーションの認証アルゴリズムを特定するために使用される。サポートされるアルゴリズムは、たとえば、ＨＭＡＣ－ＳＨＡ１、ＨＭＡＣ－ＭＤ５、ＤＥＳ－ＸＣＢＣ－ＭＡＣ、３ＤＥＳ－ＸＣＢＣ－ＭＡＣ、およびＡＥＳ－ＸＣＢＣ－ＭＡＣである。

【００６０】

マスターキー１６２６とマスターソルト１６２７は、暗号キー１６２８と認証キー１６２９が生成されていない場合に暗号処理に用いる暗号キー１６２８と認証キー１６２９とを生成するためのキー導出、または新たに受信したマスターキー１６２６に対してマスターキー再キーイングを行うために使用される。ここで、ソルトとはパスワードを複雑化するための乱数を指す。

【００６１】

暗号キー１６２８は、暗号化や復号化等のセキュアアプリケーションのための暗号処理を実行するために使用される。認証キー１６２９は、メッセージ認証またはメッセージダイジェストを実行するために使用される。

【００６２】

アプリケーション層セキュリティ処理ユニット１６４は、セキュアマルチメディアパケットの暗号化された部分を特定し、セキュアマルチメディアパケットの認証部分を特定するような、メッセージ認証の確認等のアプリケーション層セキュリティプロトコル編成を実行する。アプリケーション層セキュリティ処理ユニット１６４は、暗号化および復号化部分の特定部（locator）１６４２、認証部分および認証タグの特定部１６４６、認証タグ生成部１６４４および認証タグ確認部１６４８を含む。

【００６３】

暗号化および復号化部分の特定部１６４２は、暗号化または復号化の暗号処理で処理されるペイロードの開始アドレスと終了アドレスを特定するために使用される。ペイロードのこの特定された部分内で、暗号処理が実行される。出力リアルタイムトランスポートプロトコル（ＲＴＰ）パケットを例にとると、開始アドレスは、通常、ＲＴＰヘッダーに続く最初のバイトに一致する。終了アドレスはＲＴＰペイロードの最終バイトである。

【００６４】

認証部分および認証タグの特定部１６４６は、認証処理で処理されるペイロードの開始

アドレスと終了アドレスを特定するためにおよび認証タグを記憶するまたは読み出すための開始アドレスを特定するために使用される。ペイロードのこの特定された部分内で、認証処理が実行される。出力ＲＴＰパケットを例にとると、開始アドレスは、通常、ＲＴＰヘッダーの先頭バイトに一致する。終了アドレスはＲＴＰペイロードの最終バイトである。出力ＲＴＰパケットを例にとると、認証タグ開始アドレスは、通常、ＲＴＰペイロードの最終バイトに続く最初のバイトに一致し、認証タグは、通常、８０ビットの長さをもつ。

【００６５】

認証タグ生成部１６４４は、演算処理により得た認証タグを出力パケットのペイロードの最後に付加するために使用される。

【００６６】

認証タグ確認部１６４８は、演算処理により得た認証タグを入パケットのペイロード中の認証タグに照合して確認するために使用される。これらのタグが一致しない場合、確認は失敗しパケットを破棄する。そうではなく、これらのタグが一致する場合、セキュアマルチメディアパケットが本当に信頼できるものであり、通信相手によって真正に送信されていることを意味する。

【００６７】

暗号処理ユニット１６８は、暗号ユニット１６８２とメッセージ認証ユニット１６８４とを含む。暗号ユニット１６８２は、ＣＢＣまたはカウンターモードを含むＤＥＳ、３ＤＥＳ、ＡＥＳ、ＡＥＳ１９２、ＡＥＳ２５６などの暗号化と復号化をサポートする。

【００６８】

メッセージ認証ユニット１６８４は、たとえば、ＨＭＡＣ－ＳＨＡ１、ＨＭＡＣ－ＭＤ５、ＤＥＳ－ＸＣＢＣ－ＭＡＣ、３ＤＥＳ－ＸＣＢＣ－ＭＡＣ、およびＡＥＳ－ＸＣＢＣ－ＭＡＣのメッセージ認証処理をサポートする。

【００６９】

図５は、本発明の実施の形態による大きいサイズのセキュリティマルチメディアペイロードの構成図である。

【００７０】

セキュアマルチメディアアプリケーション１１２は、マルチメディアコンテンツを送信するためにリアルタイムトランスポートプロトコル（ＲＴＰ）を使用し、ＲＴＰヘッダー４１２と大きいサイズのペイロード４１４を含む平文のマルチメディアパケット４１０を生成する。

【００７１】

ネットワーク層の平文のマルチメディアパケット４２０は、ソケットバッファ構造体（Sk_buff構造体）４２２、ＩＰヘッダー４２４、ＵＤＰヘッダー４２６、ＲＴＰヘッダー４１２、および大きいサイズのペイロード４１４を含む。

【００７２】

アプリケーション層セキュリティプロトコルに適合するカーネルレベル暗号処理後、ネットワーク層の平文のマルチメディアパケット４２０はネットワーク層のセキュアマルチメディアパケット４３０になる。

【００７３】

ネットワーク層のセキュアマルチメディアパケット４３０は、 ソケットバッファ構造体４２２、ＩＰヘッダー４２４、ＵＤＰヘッダー４２６、ＲＴＰヘッダー４１２、暗号化された大きいサイズのペイロード４３２、およびメッセージ認証コード４３４を含む。

【００７４】

ネットワークプロトコルスタック１３０は、ネットワークインタフェース１５０のＭＴＵに応じて、大きいサイズのネットワーク層のセキュアマルチメディアパケット４３０のセグメント分割処理を実行する。

【００７５】

ネットワーク層のセキュアマルチメディアパケットのネットワークプロトコルスタック

１３０によるセグメント分割処理後、ネットワーク層のセキュアマルチメディアパケット４３０は、一連のセグメント化されたセキュアマルチメディアパケット４４０になる。一連のセグメント化されたセキュアマルチメディアパケット４４０は、第１のセグメント化されたセキュアマルチメディアパケット４４２、第１のセグメント化されたセキュアマルチメディアパケット４４４、および第ｎのセグメント化されたセキュアマルチメディアパケット４４６を含む。

【００７６】

第１のセグメント化されたセキュアマルチメディアパケット４４２は、ソケットバッファ構造体４２２、ＩＰヘッダー４２４、ＵＤＰヘッダー４２６、ＲＴＰヘッダー４１２、および第１のセグメント化された暗号化ペイロード４４２２を含む。第２のセグメント化されたセキュアマルチメディアパケット４４４は、ソケットバッファ構造４２２、ＩＰヘッダー４２４、および第２のセグメント化された暗号化ペイロード４４４２を含む。第ｎのセグメント化されたセキュアマルチメディアパケット４４６は、ソケットバッファ構造４２２、ＩＰヘッダー４２４、および第ｎのセグメント化した暗号化ペイロード４４６２を含む。

【００７７】

図６は、本発明の実施の形態に係る出力処理において様々に形態が変わるマルチメディアパケットを処理する暗号処理通信システムの一例を示す構成図である。

【００７８】

セキュアマルチメディアアプリケーション１１２は、平文のマルチメディアパケット４１０を生成し、平文のマルチメディアパケット４１０を、ソケット１１４を介して、仮想ネットワークインタフェース１４０のネットワークプロトコルスタック１３０へ送信する。

【００７９】

平文のマルチメディアパケット４１０がいったんネットワークプロトコルスタック１３０へ入力されると、ネットワーク層のパケットフォーマットの形態をとり、ネットワーク層の平文のマルチメディアパケット４２０になる。

【００８０】

出力フィルタ１３２は、ネットワーク層の平文のマルチメディアパケット４２０を選別し、カーネルレベル暗号モジュール１６０を起動して、アプリケーション層セキュリティプロトコルを実行させる。これにより、ネットワーク層の平文のマルチメディアパケット４２０はネットワーク層のセキュアマルチメディアパケット４３０になる。

【００８１】

ネットワーク層のセキュアマルチメディアパケット４３０は、仮想ネットワークインタフェース１４０に属する。

【００８２】

ネットワーク層のセキュアマルチメディアパケット４３０のＩＰヘッダー４２４中の仮想ネットワークインタフェース１４０への宛先アドレスを実際の送信先アドレスに置き換えた後、ネットワーク層のセキュアマルチメディアパケット４３０はネットワークインタフェース１５０のネットワークプロトコルスタック１３０へ送信される。

【００８３】

ネットワークインタフェース１５０のネットワークプロトコルスタック１３０へ到着すると、ネットワーク層のセキュアマルチメディアパケット４３０のセグメント分割が行われる。

【００８４】

最後に、一連のセグメント化したセキュアマルチメディアパケット４４０がネットワークインタフェース１５０から送出される。すなわち、第１のセグメント化されたセキュアマルチメディアパケット４４２、第２のセグメント化されたセキュアマルチメディアパケット４４４、第ｎのセグメント化されたセキュアマルチメディアパケット４４６は、ネットワークインタフェース１５０から送出される。

【００８５】
図７は、本発明の実施の形態による入力処理において様々に形態が変わるマルチメディアパケットを処理する暗号処理通信システムを示す構成図である。
【００８６】
一連のセグメント化されたセキュアマルチメディアパケット４４０またはネットワーク層のセキュアマルチメディアパケット４３０のいずれかがネットワーク１５０によって受信される。
【００８７】
大きいサイズのセキュアマルチメディアペイロードの場合は,第１のセグメント化されたセキュアマルチメディアパケット４４２、第２のセグメント化されたセキュアマルチメディアパケット４４４、第ｎのセグメント化されたセキュアマルチメディアパケット４４６を含む、一連のセグメント化されたセキュアマルチメディアパケット４４０がネットワーク１５０によって受信される。そうでない場合には場合は、ネットワーク層のセキュアマルチメディアパケット４３０がネットワーク１５０によって受信される。
【００８８】
ネットワークプロトコルスタック１３０にいったんパケットが到着すると、一連のセグメント化されたセキュアマルチメディアパケット４４０のネットワークプロトコルスタックによる復元処理が行われる。一連のセグメント化したセキュアマルチメディアパケット４４０は、ネットワーク層のセキュアマルチメディアパケット４３０に再組立てされる。
【００８９】
入力フィルタ１３４は、ネットワーク層のセキュアマルチメディアパケット４３０を選別し、カーネルレベル暗号モジュール１６０を起動し、復号化やメッセージ認証確認等のアプリケーション層セキュリティプロトコルを実行させる。これにより、ネットワーク層のセキュアマルチメディアパケット４３０は、ネットワーク層の平文のマルチメディアパケット４２０になる。
【００９０】
ネットワーク層の平文のマルチメディアパケット４２０は、ソケット１１４を介してセキュアマルチメディアアプリケーション１１２へ送信される。最後に、セキュアマルチメディアアプリケーション１１２は、平文のマルチメディアパケット４１０を受信する。
【００９１】
図８は、出力されるセキュアマルチメディアパケットに対してカーネルレベル暗号処理を実行するための本発明の実施の形態を示すシーケンスフローである。
【００９２】
ステップＳ３０２において、セキュアマルチメディアアプリケーション１１２は、平文のマルチメディアパケット４１０を生成する。平文のマルチメディアパケット４１０は、リアルタイムトランスポートプロトコル（ＲＴＰ）の形式で表わすことができる。
【００９３】
ステップＳ３０４において、セキュアマルチメディアアプリケーション１１２は、平文のマルチメディアパケット４１０を、ソケット１１４を介して、仮想ネットワークインタフェース１４０のネットワークプロトコルスタック１３０へ送信する。
【００９４】
ステップＳ３０６において、平文のマルチメディアパケット４１０がいったんネットワークプロトコルスタック１３０へ入力されると、ネットワーク層のパケットフォーマットの形態をとり、４２０のようなソケットバッファ構造体４２２によって表わすことができる。
【００９５】
ステップＳ３０８において、ネットワーク層の平文のマルチメディアパケット４２０は、出力フィルタリングポイント１３２に入力される。このフィルタリングポイントはネットフィルタのＮＦ_ＩＰ_ＬＯＣＡＬ_ＯＵＴであり得る。
【００９６】

ステップＳ３１０において、ＲＴＰヘッダー４１２中の３項目｛ＳＳＲＣ　ＩＤ　１６２１、送信先ネットワークアドレス１６２２、送信先トランスポートポート番号１６３４｝がフィルタリング条件に合致するので、ネットワーク層の平文のマルチメディアパケット４２０は、アプリケーション層セキュア処理情報格納部１６２中のセキュア処理情報エントリー１６２０に相当するフィルタリング条件に合致するか判定する。

【００９７】

ステップＳ３１２において、フィルタリング条件に合致する場合（Ｓ３１０：ＹＥＳ）、ネットワーク層の平文のマルチメディアパケット４２０に対するカーネルレベル暗号処理が起動される。また、フィルタリング条件に合致しない場合（Ｓ３１０：ＮＯ）、処理を終了する。

【００９８】

ステップＳ３１４において、ＲＴＰヘッダー４１２中の３項目｛ＳＳＲＣ　ＩＤ　１６２１、送信先ネットワークアドレス１６２２、送信先トランスポートポート番号１６３４｝が、暗号処理を実行するための指標として使用される。暗号キー１６２８と認証キー１６２９とが生成されていない場合は、または新たに受信したマスターキー１６２６のマスターキー再キーイングを行う場合は、暗号キー１６２８と認証キー１６２９を生成するためにマスターキー１６２６とマスターソルト１６２７が使用される。

【００９９】

暗号化の開始アドレスが、暗号化および復号化部分の特定部１６４２によって決定され、暗号化部分４３２に対する暗号化を実行するために暗号アルゴリズムＩＤ１６２４と暗号キー１６２８が使用される。

【０１００】

メッセージ認証の開始アドレスが、認証部分および認証タグの特定部１６４６によって決定され、認証部分４３２に対して認証を実行し、結果をメッセージ認証タグ４３４として保存するために、認証アルゴリズムＩＤ１６２５と認証キー１６２９が使用される。

【０１０１】

認証後、認証タグ生成部１６４４は、認証部分４３２対する認証の結果であるメッセージ認証タグ４３４をパケットに付加する。

【０１０２】

暗号化および認証後、カーネルレベル暗号モジュール１６０は、セキュアリアルタイムトランスポートプロトコル（ＳＲＴＰ）等のアプリケーション層セキュリティプロトコルに適合させることにより、ネットワーク層の平文のマルチメディアパケット４２０を、暗号化部分４３２とメッセージ認証コード４３４をもつネットワーク層のセキュアマルチメディアパケット４３０になるように修正する。

【０１０３】

ステップＳ３１６において、パケットは、セキュアリアルタイムトランスポートプロトコル（ＳＲＴＰ）等のアプリケーション層セキュリティプロトコルの適合によって暗号化部分４３２とメッセージ認証コード４３４をもつネットワーク層のパケットフォーマット４３０の形態をとる。

【０１０４】

ステップＳ３１８において、セキュアマルチメディアパケット上のネットワーク層のセキュアマルチメディアパケット４３０のＩＰヘッダー４２４中の宛先アドレスを実際の送信先アドレスに置き換えた後、ステップＳ３２０でネットワーク層のセキュアマルチメディアパケット４３０は、ネットワークインタフェース１５０のネットワークプロトコルスタック１３０へ送信される。これにより、ステップＳ３２２で、ネットワーク層のセキュアマルチメディアパケット４３０は出力フィルタリングポイント１３２を通過する。ネットワーク層のセキュアマルチメディアパケット４３０は、ネットワークインタフェース１５０のネットワークプロトコルスタック１３０へ入力される。

【０１０５】

ステップＳ３２４において、ネットワーク層のセキュアマルチメディアパケット４３０

のセグメント分割が発生するか否かの判断が行われる。ネットワーク層のセキュアマルチメディアパケット４３０がネットワークインタフェース１５０のＭＴＵよりも大きければ、この判断状態は真である。

【０１０６】

ステップＳ３２６へ進み、セグメント分割を行う。セグメント分割後、ネットワーク層のセキュアマルチメディアパケット４３０は、一連のセグメント化されたセキュアマルチメディアパケット４４０になる。その結果、７２８で、第１のセグメント化されたセキュアマルチメディアパケット４４２、第２のセグメント化されたセキュアマルチメディアパケット４４４、第ｎのセグメント化されたセキュアマルチメディアパケット４４６を含む、一連のセグメント化されたセキュアマルチメディアパケット４４０がネットワークインタフェース１５０からネットワークへ送出される。

【０１０７】

一方、ネットワーク層のセキュアマルチメディアパケット４３０がネットワークインタフェース１５０のＭＴＵよりも小さければ、判断状態は偽である。ステップＳ３２８へ進み、ネットワーク層のセキュアマルチメディアパケット４３０がネットワークインタフェース１５０からネットワークへ送出される。

【０１０８】

図９は、入力されるセキュアマルチメディアパケットに対してカーネルレベル暗号処理を実行するための本発明の実施の形態を示すシーケンスフローである。

【０１０９】

ステップＳ４０２において、ネットワークインタフェースは、セキュアマルチメディアパケット（セキュアマルチメディアパケット）を受信し、ネットワークプロトコル処理にスケジュールする。

【０１１０】

セキュアマルチメディアパケットは、第１のセグメント化されたセキュアマルチメディアパケット４４２、第２のセグメント化されたセキュアマルチメディアパケット４４４、第ｎのセグメント化されたセキュアマルチメディアパケット４４６を含む、一連のセグメント化したセキュアマルチメディアパケット４４０の形態、またはネットワーク層のセキュアマルチメディアパケット４３０の形態のいずれかであり得る。

【０１１１】

ステップＳ４０４で、セキュアマルチメディアパケットが一連のセグメント化されたセキュアマルチメディアパケット４４０の形態である場合、ネットワークインタフェース１５０のネットワークプロトコルスタック１３０は、第１のセグメント化されたセキュアマルチメディアパケット４４２、第２のセグメント化されたセキュアマルチメディアパケット４４４、第ｎのセグメント化されたセキュアマルチメディアパケット４４６を含む、一連のセグメント化したセキュアマルチメディアパケット４４０がネットワーク層のセキュアマルチメディアパケット４３０になるように復元を行う。

【０１１２】

ステップＳ４０４の後、セキュアマルチメディアパケットは、ソケットバッファ構造４２２の形式によって表わされるネットワーク層のセキュアマルチメディアパケット４３０になる。

【０１１３】

ステップＳ４０６において、ネットワーク層のセキュアマルチメディアパケット４３０は、入力フィルタリングポイント１３４へ入力される。このフィルタリングポイントは、ネットフィルタのＮＦ_ＩＰ_ＬＯＣＡＬ_ＩＮであり得る。

【０１１４】

ステップＳ４０８において、ＲＴＰヘッダー４１２中の３項目｛ＳＳＲＣ　ＩＤ１６２１、送信先ネットワークアドレス１６２２、送信先トランスポートポート番号１６３４｝がフィルタリング条件に合致するので、ネットワーク層のセキュアマルチメディアパケット４３０は、アプリケーション層セキュア処理情報格納部１６２中のセキュア処理情報エ

ントリー１６２０に相当するフィルタリング条件に合致する。
【０１１５】
ステップＳ４１０において、フィルタリング条件に合致する場合（Ｓ４０８：ＹＥＳ）、ネットワーク層のセキュアマルチメディアパケット４３０に対するカーネルレベル暗号処理は、起動される。フィルタリング条件に合致する場合（Ｓ４０８：ＮＯ）、処理を終了する。
【０１１６】
ステップＳ４１２において、ＲＴＰヘッダー４１２中の３項目｛ＳＳＲＣ　ＩＤ１６２１、送信先ネットワークアドレス１６２２、送信先トランスポートポート番号１６３４｝は、暗号処理を実行するための指標として使用される。
【０１１７】
暗号キー１６２８と認証キー１６２９が生成されていない場合、または新たに受信したマスターキー１６２６のマスターキー再キーイングを行う場合は、暗号キー１６２８と認証キー１６２９を生成するためにマスターキー１６２６とマスターソルト１６２７が使用される。
【０１１８】
復号化の開始アドレスが、暗号化および復号化部分の特定部１６４２によって決定され、復号化部分４３２に対する復号化を実行するために暗号アルゴリズムＩＤ１６２４と暗号キー１６２８が使用される。
【０１１９】
メッセージ認証の開始アドレスが、認証部分および認証タグの特定部１６４６によって決定され、認証部分４３２に対して認証を実行するために、認証アルゴリズムＩＤ１６２５と認証キー１６２９が使用される。この結果は演算処理されたメッセージ認証という。
【０１２０】
ステップＳ４１４において、演算処理されたメッセージ認証がメッセージ認証コード４３４に厳密に一致するか否かを確認するために、認証タグ確認部１６４８が使用される。
【０１２１】
これらが厳密に一致する場合、ネットワーク層のセキュアマルチメディアパケット４３０は本当に信頼できるものであり、通信相手によって真正に送信されていることを意味する。
【０１２２】
これらが厳密に一致しない場合、ネットワーク層のセキュアマルチメディアパケット４３０は偽物であることを意味し、フローはステップＳ４１６へ進み、ネットワーク層のセキュアマルチメディアパケット４３０を廃棄する。
【０１２３】
これらが厳密に一致する場合、フローはステップＳ４１８へ進み、復号化部分４３２とメッセージ認証コード４３４をもつネットワーク層のセキュアマルチメディアパケット４３０がリアルタイムトランスポートプロトコル（ＲＴＰ）に適合するネットワーク層の平文のマルチメディアパケット４２０になるようにセキュアマルチメディアパケット４３０のペイロードを修正する。
【０１２４】
ステップＳ４２０において、ネットワーク層の平文のマルチメディアパケット４２０は前記入力フィルタリングポイント１３４を通過する。
【０１２５】
ステップＳ４２２において、ソケットバッファ構造体４２２の形式によって表わされる、ネットワーク層の平文のマルチメディアパケット４２０は、ソケット１１４によってセキュアマルチメディアアプリケーション１１２へ送信される。
【０１２６】
最後に、ステップＳ４２４において、平文のマルチメディアパケット４１０がソケット１１４から受信され、マルチメディアコンテンツがＲＴＰペイロード４１４から取り出さ

れる。

【０１２７】

このように、本実施の形態によれば、セグメント分割の問題を避けるために比較的大きな最大送信単位（ＭＴＵ）をもつ仮想ネットワークインタフェースへ大きいサイズのペイロードを送信し、仮想ネットワークインタフェースのネットワークプロトコルスタックにいったん取り込んだ大きいサイズのペイロード全体に対して、カーネルレベルの暗号処理を起動し、セキュア化されたペイロードをネットワークインタフェースのネットワークプロトコルスタックへ送信することにより、既存のネットワークプロトコルスタックを生かしつつ、最低限のメモリコピー回数でアプリケーション層セキュアプロトコル処理を実現することが可能になる。

【産業上の利用可能性】

【０１２８】

本発明の暗号処理装置は、セキュアマルチメディア通信の暗号処理性能を効果的に増進する暗号処理装置として有用である。

【図面の簡単な説明】

【０１２９】

【図１】本発明の実施の形態を示す暗号処理通信システムの構成図

【図２】出力されるセキュアマルチメディアパケットに対してカーネルレベル暗号処理を実行するための本発明の実施の形態を示すフローチャート

【図３】入力されるセキュアマルチメディアパケットに対してカーネルレベル暗号処理を実行するための本発明の実施の形態を示すフローチャート

【図４】セキュアマルチメディアアプリケーションの統制部、アプリケーション層セキュア処理情報、アプリケーション層セキュリティ処理ユニット、および暗号処理ユニットの構成図

【図５】本発明の実施の形態による大きいサイズのセキュリティマルチメディアペイロードの構成図

【図６】本発明の実施の形態による出力処理において様々に形態が変わるマルチメディアパケットを処理する暗号処理通信システムを示す構成図

【図７】本発明の実施の形態による入処理において様々に形態が変わるマルチメディアパケットを処理する暗号処理通信システムを示す構成図

【図８】出力されるセキュアマルチメディアパケットに対してカーネルレベル暗号処理を実行するための本発明の実施の形態を示すシーケンスフロー

【図９】入力されるセキュアマルチメディアパケットに対してカーネルレベル暗号処理を実行するための本発明の実施の形態を示すシーケンスフロー

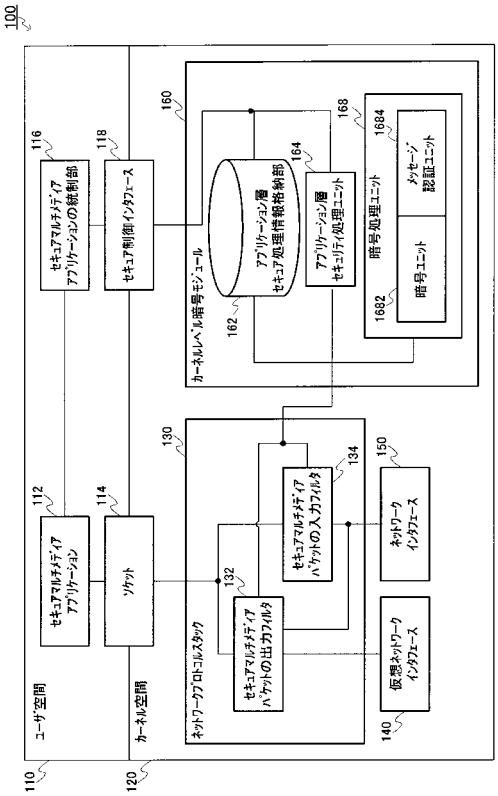
【符号の説明】

【０１３０】

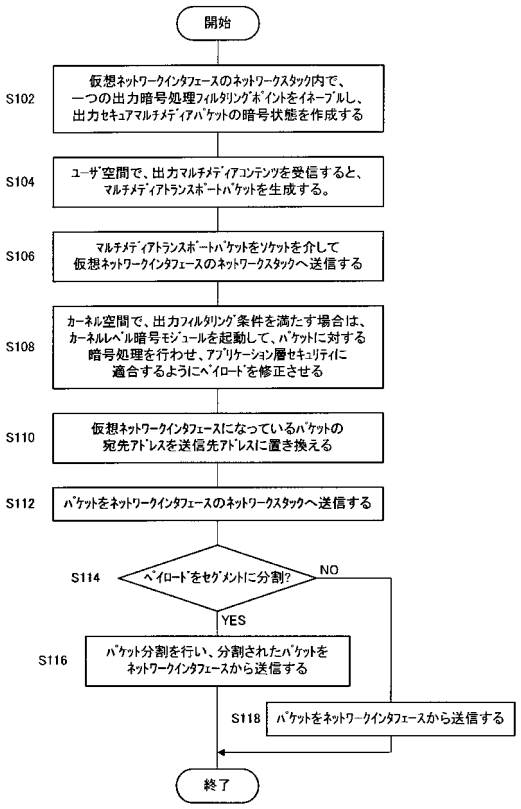
１１０　ユーザ空間
１１４　ソケット
１２０　カーネル空間
１１２　セキュアマルチメディアアプリケーション
１１６　セキュアマルチメディアアプリケーションの統制部
１１６２　セキュアアプリケーションセッションの開始ユニット
１１６４　セキュアアプリケーションセッションの終了ユニット
１１８　セキュア制御インタフェース
１３０　ネットワークプロトコルスタック
１３２　セキュアマルチメディアパケットの出力フィルタ
１３４　セキュアマルチメディアパケットの入力フィルタ
１４０　仮想ネットワークインタフェース
１５０　ネットワークインタフェース
１６０　カーネルレベル暗号モジュー

１６２　アプリケーション層セキュア処理情報格納部
１６２０　セキュア処理情報のエントリー
１６２２　送信先ネットワークアドレス
１６２３　送信先トランスポートポート番号
１６２４　暗号アルゴリズムＩＤ
１６２５　認証アルゴリズムＩＤ
１６２６　マスターキー
１６２７　マスターソルト
１６２８　暗号キー
１６２９　認証キー
１６４　アプリケーション層セキュリティ処理ユニット
１６４２　暗号化および復号化部分の特定部
１６４４　認証タグ生成部
１６４６　認証部分および認証タグの特定部
１６４８　認証タグ確認部
１６８　暗号処理ユニット
１６８２　暗号ユニット
１６８４　メッセージ認証ユニット
４１２　ＲＴＰヘッダー
４１４　マルチメディアコンテンツを運ぶための大きいサイズのペイロード
４２４　ＩＰヘッダー
４２６　ＵＤＰヘッダー
４１２　ＲＴＰヘッダー
４３２　マルチメディアコンテンツを運ぶための大きいサイズのペイロード
４３４　メッセージ認証コード

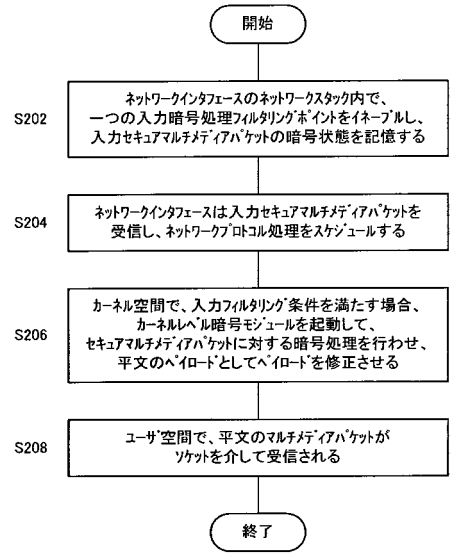
【図１】



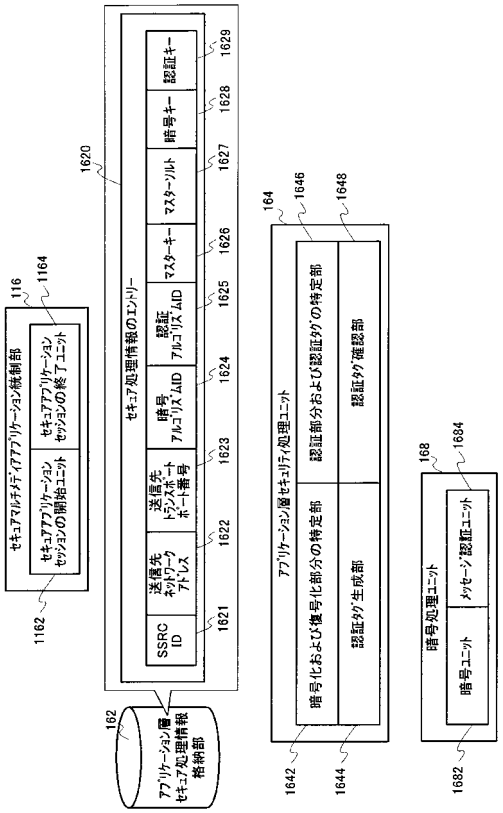
【図２】



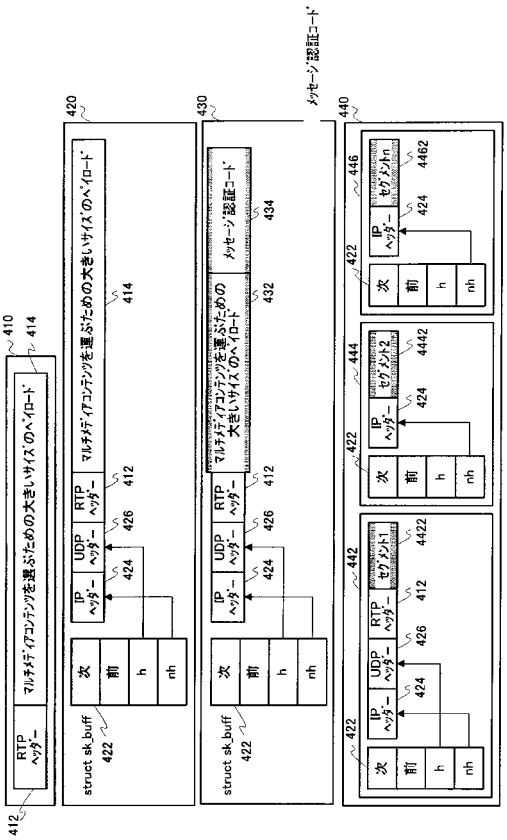
【図３】


開始
S202
ネットワークインタフェースのネットワークスタック内で、
一つの入力暗号処理フィルタリングポイントをイネーブルし、
入力セキュアマルチメディアパケットの暗号状態を記憶する
S204
ネットワークインタフェースは入力セキュアマルチメディアパケットを
受信し、ネットワークプロトコル処理をスケジュールする
S206
カーネル空間で、入力フィルタリング条件を満たす場合、
カーネルレベル暗号モジュールを起動して、
セキュアマルチメディアパケットに対する暗号処理を行わせ、
平文のペイロードとしてペイロードを修正させる
S208
ユーザ空間で、平文のマルチメディアパケットが
ソケットを介して受信される
終了

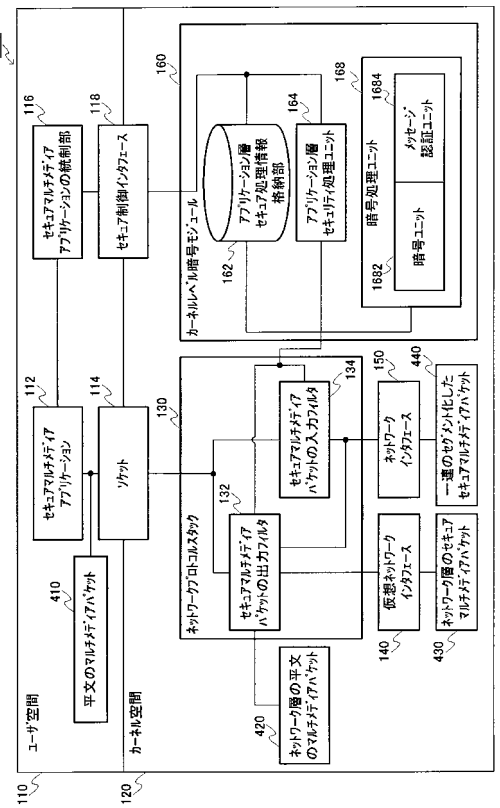
【図４】


セキュアマルチメディアアプリケーション統制部
セキュアアプリケーション
セッションの開始ユニット
セキュアアプリケーション
セッションの終了ユニット
セキュア処理情報のエントリー
SSRC ID
送信先 ネットワーク アドレス
送信先 トランスポート ポート番号
暗号 アルゴリズム/ID
認証 アルゴリズム/ID
マスターキー
マスターソルト
暗号キー
認証キー
アプリケーション層 セキュア処理情報 格納部
アプリケーション層セキュリティ処理ユニット
暗号化および複号化部分の特定部
認証部分および認証タグの特定部
認証タグ生成部
認証タグ確認部
暗号処理ユニット
暗号ユニット
メッセージ認証ユニット

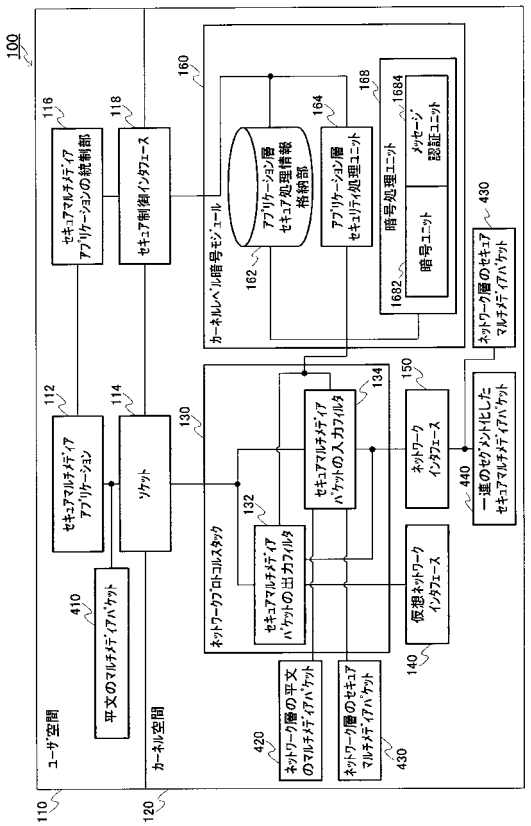
【図５】


メッセージ認証コード
RTP ヘッダー
マルチメディアコンテンツを運ぶための大きいサイズのペイロード
struct sk_buff
IP ヘッダー
UDP ヘッダー
RTP ヘッダー
次
前
h
nh
セグメント1
セグメント2

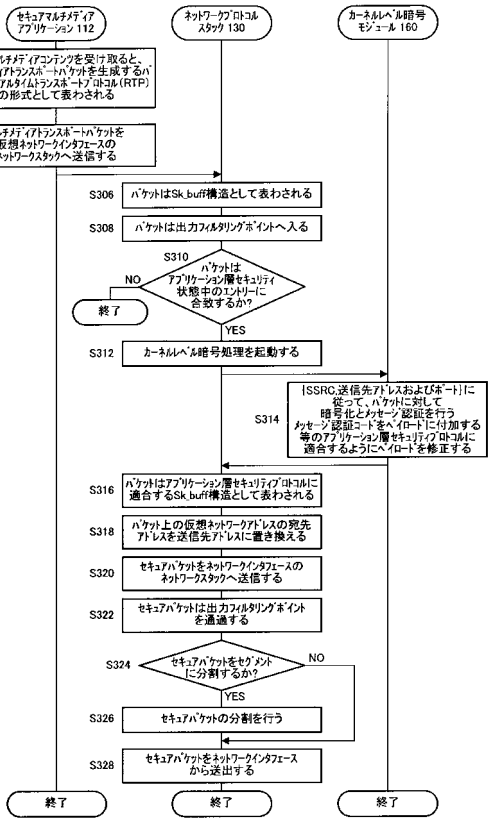
【図６】


ユーザ空間
カーネル空間
セキュアマルチメディアアプリケーション
セキュアマルチメディアアプリケーションの統制部
セキュア制御インタフェース
ソケット
ネットワークプロトコルスタック
セキュアマルチメディアパケットの出力フィルタ
セキュアマルチメディアパケットの入力フィルタ
ネットワークインタフェース
仮想ネットワークインタフェース
平文のマルチメディアパケット
ネットワーク層の平文のマルチメディアパケット
ネットワーク層のセキュアマルチメディアパケット
一連のサブメントに化したセキュアマルチメディアパケット
カーネルレベル暗号モジュール
アプリケーション層セキュア処理情報格納部
アプリケーション層セキュリティ処理ユニット
暗号処理ユニット
暗号ユニット
メッセージ認証ユニット

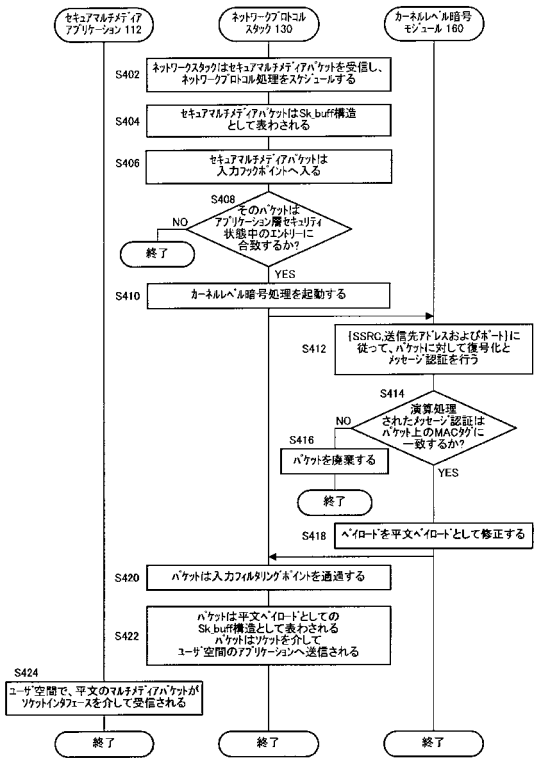
【図７】


100
セキュアマルチメディアアプリケーションの統制部
セキュア制御インタフェース
カーネルレベル暗号モジュール
アプリケーション層セキュア処理情報格納部
アプリケーション層セキュリティ処理ユニット
暗号処理ユニット
メッセージ認証ユニット
暗号ユニット
ネットワーク層のセキュアマルチメディアパケット
セキュアマルチメディアアプリケーション
ソケット
ネットワークプロトコルスタック
セキュアマルチメディアパケットの入力フィルタ
セキュアマルチメディアパケットの出力フィルタ
ネットワークインタフェース
仮想ネットワークインタフェース
一連のセグメント化したセキュアマルチメディアパケット
平文のマルチメディアパケット
ネットワーク層の平文のマルチメディアパケット
ネットワーク層のセキュアマルチメディアパケット
ユーザ空間
カーネル空間
110
120
116
118
160
164
168
1684
162
1682
430
112
114
130
134
150
132
410
140
420
430

【図８】


セキュアマルチメディアアプリケーション 112
ネットワークプロトコルスタック 130
カーネルレベル暗号モジュール 160
S302
出力マルチメディアコンテンツを受け取ると、マルチメディアトランスポートパケットを生成するパケットはリアルタイムトランスポートプロトコル(RTP)の形式として表わされる
S304
マルチメディアトランスポートパケットを仮想ネットワークインタフェースのネットワークスタックへ送信する
S306
パケットはSk_buff構造として表わされる
S308
パケットは出力フィルタリングポイントへ入る
S310
パケットはアプリケーション層セキュリティ状態中のエントリーに合致するか?
NO
終了
YES
S312
カーネルレベル暗号処理を起動する
S314
{SSRC,送信先アドレスおよびポート}に従って、パケットに対して暗号化とメッセージ認証を行うメッセージ認証コードをペイロードに付加する等のアプリケーション層セキュリティプロトコルに適合するようにペイロードを修正する
S316
パケットはアプリケーション層セキュリティプロトコルに適合するSk_buff構造として表わされる
S318
パケット上の仮想ネットワークアドレスの宛先アドレスを送信先アドレスに置き換える
S320
セキュアパケットをネットワークインタフェースのネットワークスタックへ送信する
S322
セキュアパケットは出力フィルタリングポイントを通過する
S324
セキュアパケットをセグメントに分割するか?
NO
YES
S326
セキュアパケットの分割を行う
S328
セキュアパケットをネットワークインタフェースから送出する
終了
終了
終了

【図９】


セキュアマルチメディアアプリケーション 112
ネットワークプロトコルスタック 130
カーネルレベル暗号モジュール 160
S402
ネットワークスタックはセキュアマルチメディアパケットを受信し、ネットワークプロトコル処理をスケジュールする
S404
セキュアマルチメディアパケットはSk_buff構造として表わされる
S406
セキュアマルチメディアパケットは入力フックポイントへ入る
S408
そのパケットはアプリケーション層セキュリティ状態中のエントリーに合致するか?
NO
終了
YES
S410
カーネルレベル暗号処理を起動する
S412
{SSRC,送信先アドレスおよびポート}に従って、パケットに対して復号化とメッセージ認証を行う
S414
演算処理されたメッセージ認証はパケット上のMACタグに一致するか?
NO
S416
パケットを廃棄する
終了
YES
S418
ペイロードを平文ペイロードとして修正する
S420
パケットは入力フィルタリングポイントを通過する
S422
パケットは平文ペイロードとしてのSk_buff構造として表わされるパケットはソケットを介してユーザ空間のアプリケーションへ送信される
S424
ユーザ空間で、平文のマルチメディアパケットがソケットインタフェースを介して受信される
終了
終了
終了

フロントページの続き

(72)発明者　フォン　チェン　ウェ
台湾１０６５７台北市大安区仁愛路３段１３６号１０楼１００２室　パナソニック台湾研究所内

審査官　青木　重徳

(56)参考文献　特開２００５－２２９６５２（ＪＰ，Ａ）
特開２００４－１９９３１５（ＪＰ，Ａ）
特開平１０－１９０６４９（ＪＰ，Ａ）
特表２００５－５１４７０３（ＪＰ，Ａ）
国際公開第２００７／０２３４６７（WO，Ａ１）
稲村　雄，本郷　節之，“暗号技術によるメモリデータ保護方式の提案”，情報処理学会論文誌，日本，社団法人情報処理学会，２００４年　8月１５日，第４５巻，第8号，ｐ．１８２３－１８３２

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３６
Ｈ０４Ｌ　１２／２２