(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2004-247810
(P2004-247810A)
(43)公開日　平成16年9月2日(2004.9.2)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/32	H04L 9/00	675A	5J104
G09C 1/00	G09C 1/00	640D	
H04L 9/08	H04L 9/00	685	
H04L 9/36	H04L 9/00	601C	
	H04L 9/00	601E	

審査請求 未請求　請求項の数 12　ＯＬ　（全 14 頁）

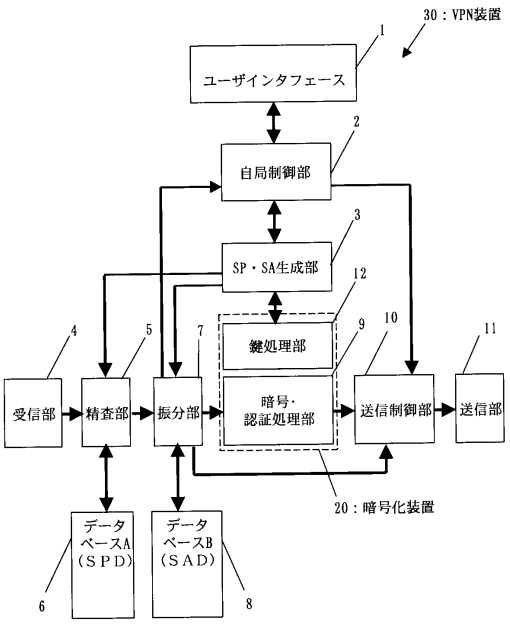
(21)出願番号　特願2003-33342(P2003-33342)
(22)出願日　平成15年2月12日(2003.2.12)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100111800
弁理士　竹内　三明
(74)代理人　100114878
弁理士　山地　博人
(72)発明者　竹内　清史
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

Ｆターム(参考)　5J104 AA01 AA08 AA16 AA18 EA04 EA18 JA01 LA01 NA02 NA12 NA20 NA38 PA07

(54)【発明の名称】暗号化装置及び通信装置及び復号装置及び暗号化方法及び復号方法及び暗号化プログラム及び復号プログラム

(57)【要約】
【課題】本発明は、ＶＰＮ装置のスループットを向上させる暗号化装置及び復号装置及びその方法を提供することを目的とする。
【解決手段】HMAC処理によりＩＰＳＥＣ認証処理を行うＶＰＮ装置３０において、ＶＰＮ装置３０に含まれる暗号化装置２０に認証鍵データに対するハッシュ処理のみを先に実行する鍵処理部１２を設け、ハッシュした結果（中間鍵ａ、中間鍵ｂ）を認証鍵の代わりに中間鍵をデータベースＢ（ＳＡＤ）８に記憶し、HMAC処理にて繰り返し認証鍵データのハッシュ処理を行う代わりに、データベースＢ（ＳＡＤ）８に記憶してあるハッシュ結果のデータ（中間鍵ａ、中間鍵ｂ）を読み出して使うことにより、ＩＰＳＥＣ認証処理対象パケットごとに実行することが必要であった認証鍵データのハッシュ処理を１回で済むようにする。
【選択図】　図１



【特許請求の範囲】
【請求項１】
鍵に関する所定のデータから中間鍵を生成する鍵処理部と、
上記鍵処理部が生成した中間鍵を記憶するデータベースと、
パケットに含まれるメッセージを暗号化するとともに上記データベースに記憶した中間鍵を認証鍵として使用して暗号化したメッセージを認証する暗号・認証処理部とを備えた暗号化装置。
【請求項２】
鍵に関する情報を記憶するデータベースと、
鍵に関する所定のデータから中間鍵を生成し、生成した中間鍵を上記データベースに記憶し、パケットに含まれるメッセージを暗号化するとともに上記データベースに記憶した中間鍵を認証鍵として繰り返し使用してメッセージを認証する暗号・認証処理部とを備えた暗号化装置。
【請求項３】
上記暗号・認証処理部は、上記データベースに記憶した中間鍵を繰り返し使用して複数のパケットに含まれるメッセージを認証する請求項１または請求項２のいずれかに記載された暗号化装置。
【請求項４】
鍵に関する所定のデータから中間鍵を生成し、複数のパケットの第１のパケットに含まれるメッセージを暗号化し、生成した中間鍵を使用して暗号化したメッセージを認証するとともに生成した中間鍵を中間鍵メモリに記憶し、上記複数のパケットの第１のパケット以外のパケットに含まれるメッセージを暗号化するとともに中間鍵メモリに記憶した中間鍵を繰り返し使用して認証する暗号・認証処理部を備えた暗号化装置。
【請求項５】
上記暗号・認証処理部は、上記中間鍵をハッシュ関数に代入することによりメッセージを認証する請求項１または請求項２または請求項４のいずれかに記載された暗号化装置。
【請求項６】
上記暗号化装置は、上記暗号・認証処理部が認証したメッセージを含むパケットの通信をＩＰＳＥＣプロトコル（ＩＰ　ＳＥＣＵＲＩＴＹ　ＰＲＯＴＯＣＯＬ）に準拠して行うことでＶＰＮ（ＶＩＲＴＵＡＬ　ＰＲＩＶＡＴＥ　ＮＥＴＷＯＲＫ）によるパケット通信を行う請求項１または請求項２または請求項４のいずれかに記載された暗号化装置。
【請求項７】
鍵に関する所定のデータから中間鍵を生成する鍵処理部と、
上記鍵処理部が生成した中間鍵を記憶するデータベースと、
パケットに含まれるメッセージを暗号化するとともに上記データベースに記憶した中間鍵を認証鍵として使用して暗号化したメッセージを認証する暗号・認証処理部と、
上記暗号・認証処理部によって認証されたメッセージを含むパケットを送信する送信部を備えた通信装置。
【請求項８】
鍵に関する所定のデータから中間鍵を生成する鍵処理部と、
上記鍵処理部が生成した中間鍵を記憶するデータベースと、
パケットに含まれるメッセージを復号するとともに上記データベースに記憶した中間鍵を認証鍵として繰り返し使用して復号したメッセージを認証する復号・認証処理部とを備えた復号装置。
【請求項９】
鍵に関する所定のデータから中間鍵を生成し、
上記生成した中間鍵をデータベースに記憶し、
パケットに含まれるメッセージを暗号化するとともに上記データベースに記憶した中間鍵を認証鍵として使用して暗号化したメッセージを認証する暗号化方法。
【請求項１０】

鍵に関する所定のデータから中間鍵を生成し、
上記生成した中間鍵をデータベースに記憶し、
パケットに含まれるメッセージを復号するとともに上記データベースに記憶した中間鍵を認証鍵として繰り返し使用して復号したメッセージを認証する復号方法。
【請求項１１】
鍵に関する所定のデータから中間鍵を生成する処理と、
上記生成した中間鍵をデータベースに記憶する処理と、
パケットに含まれるメッセージを暗号化するとともに上記データベースに記憶した中間鍵を認証鍵として使用して暗号化したメッセージを認証する処理とをコンピュータに実行させる暗号化プログラム。
【請求項１２】
鍵に関する所定のデータから中間鍵を生成する処理と、、
上記生成した中間鍵をデータベースに記憶する処理と、
パケットに含まれるメッセージを復号するとともに上記データベースに記憶した中間鍵を認証鍵として繰り返し使用して復号したメッセージを認証する処理とをコンピュータに実行させる復号プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、パケットを認証処理する暗号化装置及び復号装置に関する。
【０００２】
【従来の技術】
パケットのＩＰＳＥＣ（ＩＰ　ＳＥＣＵＲＩＴＹ）処理方式はＩＥＴＦ（ＩＮＴＥＲＮＥＴ　ＥＮＧＩＮＥＥＲＩＮＧ　ＴＡＳＫ　ＦＯＲＣＥ）による仕様書ＲＦＣ（ＲＥＱＵＥＳＴ　ＦＯＲ　ＣＯＭＭＥＮＴＳ）２４０２にて「ＩＰ認証ヘッダ（ＡＨ）」、ＲＦＣ２４０６にて「ＩＰ暗号ペイロード（ＥＳＰ）」について記述されている。
【０００３】
ＩＰＳＥＣを通信装置に実装する上でサポートしなければならない認証処理方式はＨＭＡＣ（ＫＥＹＥＤ－ＨＡＳＨＩＮＧ　ＦＯＲ　ＭＥＳＳＡＧＥ　ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ）であり、ＨＭＡＣ処理中のハッシュ関数に使用される認証アルゴリズムは、ＭＤ５もしくはＳＨＡ１である。
【０００４】
従来のＨＭＡＣ処理の流れについて説明する。
まず、認証鍵Ｋに０をパディングし、使用するハッシュ関数のブロックサイズに合わせ、これとｉｐａｄの排他的論理和を行いＩＫ１を生成する（ステップ１）。
次にＩＫ１の後ろにＨＭＡＣ処理対象データＰを付加し、さらにパディングデータ　ＰＡＤ　ＤＡＴＡ、データ長Ｌを付加し、ハッシュ関数のブロックサイズの倍数となるハッシュ処理対象データＩＰ１を生成する（ステップ２）。
次に、ハッシュ関数ＨによるＩＰ１のハッシュ処理を行い、ダイジェストＤ１を生成する（ステップ３）。
次に、ステップ１と同様、認証鍵Ｋに０をパディングし、使用するハッシュ関数のブロックサイズにあわせ、これとｏｐａｄの排他的論理和を行い、ＩＫ２を生成する（ステップ４）。
次に、ＩＫ２の後ろにステップ３の結果得られたダイジェストＤ１を付加し、さらにパディングデータＰＡＤ　ＤＡＴＡ、データ長Ｌを追加し、ハッシュ関数の２ブロックサイズになるハッシュ処理対象データＩＰ２を生成する（ステップ５）。
次に、ハッシュ関数ＨによるＩＰ２のハッシュ処理を行い、ダイジェストＤ２を生成する。最終的にＤ２の上位９６ｂｉｔがＩＰＳＥＣパケットの認証ダイジェストとして付加される（ステップ６）。
【０００５】

次に、上記ステップ３のハッシュ処理の詳細を説明する。
ハッシュ処理はハッシュ初期値、ハッシュ処理対象データを用いて１ブロックずつ行う。
まず、ハッシュ初期値はハッシュ関数ＭＤ５、ハッシュ関数ＳＨＡ１で定義されているハッシュ初期値Ｈ０を用い、被ハッシュデータをＩＫ１として１ブロックサイズのハッシュ処理を行い、ＭＫ１を生成する（鍵ブロックのハッシュ処理１）。
次に、ハッシュ初期値としてＭＫ１を用い、被ハッシュデータをＩＰ１におけるＩＫ１の後ろの１ブロック分ＩＰ１（１）として１ブロックサイズのハッシュ処理を行い、ＭＰ１（１）を生成する（平文ブロックのハッシュ処理１）。
次に、ハッシュ処理対象データ分の処理が完了したかどうか判定し、未処理のハッシュ処理対象データがある場合は上述した「平文ブロックのハッシュ処理１」を繰り返し行う。
ここで「平文ブロックのハッシュ処理１」におけるハッシュ初期値は前回の「平文ブロックのハッシュ処理１」の結果ＭＰ１（Ｎ－１）とする。
ハッシュ処理対象データ分の処理が完了されたと判断した場合は最終的に得たＭＰ１（Ｎ）をＤ１として終了する。

【０００６】

次に、上記ステップ６のハッシュ処理の詳細を説明する。
上記ステップ３のハッシュ処理と同様、ハッシュ初期値はハッシュ関数ＭＤ５、ＳＨＡ１で定義されているハッシュ初期値Ｈ０を用い、被ハッシュデータをＩＫ２として１ブロックサイズのハッシュ処理を行いＭＫ２を生成する（鍵ブロックのハッシュ処理２）。
次に、ハッシュ初期値としてＭＫ２を用い、被ハッシュデータをＩＰ２（１）として１ブロックサイズのハッシュ処理を行い、この結果をＤ２とする（平文ブロックのハッシュ処理２）。

【０００７】

上のハッシュ処理において時間を要するのはステップ３、ステップ６であり、その処理時間はハッシュ処理対象データのブロックサイズに比例して増加する。

【０００８】

次にハッシュ処理のデータ長について述べる。ＳＨＡ１、ＭＤ５共に１ブロック＝５１２ｂｉｔである。あるデータに対してハッシュ処理を行う場合、このハッシュ処理対象データの後ろにパディングデータ（１～５１２ｂｉｔ）、データ長（６４ｂｉｔ）が付加される。
パディングデータは、ハッシュ処理対象データ、パディングデータ、データ長を合わせたデータサイズを５１２ｂｉｔの倍数に合わせるためのものであり、データ長はパディングビット付加前のハッシュ処理対象データ長を示す。

【０００９】

次にハッシュ処理時間について述べる。ハッシュ処理に要する時間は、パディングデータ、データ長付加前のハッシュ処理対象データ長が１ｂｉｔ～４４７ｂｉｔの場合１ブロック分、４４８ｂｉｔ～９５９（４４７＋５１２）ｂｉｔの場合２ブロック分、以後５１２ｂｉｔ刻みにつき１ブロック分ずつ増えていくことになる。
これによりＨＭＡＣ処理中の認証アルゴリズムによるハッシュ処理のステップ３とステップ６の処理時間は、ハッシュ処理対象データ長のブロックサイズに比例して増加する。

【００１０】

短パケットを例にしてＨＭＡＣ処理時間について述べる。
短パケットに対しＩＰＳＥＣ認証処理する場合、ＨＭＡＣ処理適用範囲はＥＳＰで４４８ｂｉｔ、ＡＨで６２４ｂｉｔである。
これについてＨＭＡＣ処理を行った場合、パケットのＨＭＡＣ処理適用範囲のハッシュ処理（平文ブロックのハッシュ処理１）で２ブロック分、認証鍵のハッシュ処理（鍵ブロックのハッシュ処理１、鍵ブロックのハッシュ処理２）で２ブロック分、最終的に認証ダイジェストを求めるハッシュ処理（平文ブロックのハッシュ処理２）で１ブロック分の合計５ブロック分を必要とする。

【００１１】

一般的に考えられるＶＰＮ（ＶＩＲＴＵＡＬ　ＰＲＩＶＡＴＥ　ＮＥＴＷＯＲＫ）装置の暗号側の構成を説明する。
暗号側のＶＰＮ装置は、ユーザインタフェースと、自局端末としての機能を実現し、自局端末宛のパケットを振分部より受け取り、自局端末発のパケットを送信制御部に渡し、ユーザインタフェースより設定されたＶＰＮの設定情報をＳＰ・ＳＡ生成部に渡す自局制御部と、ＶＰＮの設定情報、他ＶＰＮ装置と相互通信して受け取った情報を自局制御部より受け取り、これらの情報からＳＰ（ＳＥＣＵＲＩＴＹ　ＰＯＬＩＣＹ）データ、ＳＡ（ＳＥＣＵＲＩＴＹ　ＡＳＳＯＣＩＡＴＩＯＮ）データを生成して、ＳＰデータを精査部に、ＳＡデータを振分部７に渡すＳＰ・ＳＡ生成部と、パケットを受信する受信部と、ＳＰデータをＳＰＤ　６（ＳＥＣＵＲＩＴＹ　ＰＯＬＩＣＹ　ＤＡＴＡＢＡＳＥ）に登録し、パケットの精査を行う精査部と、ＳＰデータを保存するデータベースであるＳＰＤと、ＳＡデータをＳＡＤ（ＳＥＣＵＲＩＴＹ　ＡＳＳＯＣＩＡＴＩＯＮ　ＤＡＴＡＢＡＳＥ）に登録し、自局宛パケットを自局制御部に、ＩＰＳＥＣ対象外パケットを送信制御部に、ＩＰＳＥＣ処理対象パケットを暗号・認証処理部に、またこのときＳＡＤよりＳＡデータを読み出して暗号・認証処理部に渡す振分部と、ＳＡデータを保存するデータベースであるＳＡＤと、パケットのＩＰＳＥＣ処理を行う暗号・認証処理部と、自局制御部、暗号・認証処理部、振分部より受け取った送信パケットの宛先を制御する送信制御部と、パケットを送信する送信部とから構成される。

【００１２】
次にこの一般的なＶＰＮ装置における暗号側の処理の流れを説明する。
パケット処理の前準備として、まずはＳＰデータ、ＳＡデータを生成して、それぞれＳＰＤ、ＳＡＤに登録し、その後パケットのＩＰＳＥＣ処理を行う。

【００１３】
まずＳＰデータ、ＳＡデータを生成するために、ＶＰＮ管理者がＶＰＮ装置自局端末のユーザインタフェースを介してＶＰＮ装置の設定を行い、自局制御部はユーザインタフェースから受け取った情報をＳＰ・ＳＡ生成部に渡し、ＳＰ・ＳＡ生成部はＳＰデータを生成後、これを精査部に渡し、精査部はＳＰデータをＳＰＤに登録する。

【００１４】
次に、装置間でＶＰＮを構築するため、装置間で相互通信を行いＳＡデータを生成する。
ＳＰ・ＳＡ生成部は、ＳＡデータを決定するための他ＶＰＮ装置宛のデータを自局制御部に渡し、自局制御部はこれをパケット化して送信制御部に渡し、送信制御部は送信部に渡し、送信部はこれを装置外に送信する。受信部は他ＶＰＮ装置からのＳＡデータを決定するための情報を持つ受信パケットを精査部に渡し、精査部は振分部に渡し、振分部は自局宛と判断し、このパケットを自局制御部に渡し、自局制御部はこれをＳＰ・ＳＡ生成部に渡す。
以上の通信によりＳＡデータを決定したら、ＳＰ・ＳＡ生成部はＳＡデータを振分部に渡し、振分部はこれをＳＡＤに登録する。

【００１５】
次に受信部はＩＰＳＥＣ処理対象パケットを受信し、精査部に渡す。精査部は、パケットヘッダの発信元アドレス、宛先アドレス、プロトコル、ポート番号を元に、このパケットはＩＰＳＥＣ処理対象であると判断し、ＳＰＤよりこのパケットに対応するＳＰＩ（ＳＥＣＵＲＩＴＹ　ＰＡＲＡＭＥＴＥＲ　ＩＮＤＥＸ）を読み出し、これとパケットを振分部に渡す。振分部はＳＰＩを元にＳＡＤを参照して、暗号アルゴリズム、認証アルゴリズム、暗号鍵、認証鍵といったＳＡデータを暗号・認証処理部に渡す。
暗号・認証処理部はＳＡデータに含まれる処理情報を元にパケットのＩＰＳＥＣ処理を行い、処理後のパケットを送信制御部に渡す。ここで、ＳＡデータで示された処理が認証処理を含む場合、暗号・認証処理部はパケットのＨＭＡＣ処理を行う。送信制御部は、暗号・認証処理部から受け取ったパケットが他ＶＰＮ装置宛であると判断し、これを送信部に渡す。送信部はパケットを装置の外へ送信する（例えば、特許文献１参照）。

【００１６】

【特許文献１】
特開平１１－８６２０号公報
【００１７】
【発明が解決しようとする課題】
上記のようなＶＰＮ装置構成の場合、ＨＭＡＣ処理を全て暗号・認証処理部で行うことになる。ＨＭＡＣ処理には、パケットデータを必要とせず、認証鍵データを必要とするハッシュ処理部分が存在する（鍵ブロックのハッシュ処理１、鍵ブロックのハッシュ処理２）。これをＨＭＡＣ鍵処理とする。
同一の認証鍵を使用するパケットが複数存在した場合、ＨＭＡＣ鍵処理がパケットごとに実行されるので時間がかかり非効率であるという問題があった。
【００１８】
本発明は、ＶＰＮ装置のスループットを向上させる暗号化装置及び復号装置及びその方法を提供することを目的とする。
【００１９】
【課題を解決するための手段】
本発明に係る暗号化装置は、
鍵に関する所定のデータから中間鍵を生成する鍵処理部と、
上記鍵処理部が生成した中間鍵を記憶するデータベースと、
パケットに含まれるメッセージを暗号化するとともに上記データベースに記憶した中間鍵を認証鍵として使用して暗号化したメッセージを認証する暗号・認証処理部とを備える。
【００２０】
【発明の実施の形態】
実施の形態１．
実施の形態１について説明する。
図１は、本実施の形態１の発明を示したＶＰＮ装置３０のシステム構成図である。ＶＰＮ装置３０は、本発明の暗号化装置２０に通信機能及びインタフェース機能を付加した通信装置の一例である。
図１において、自局制御部２は、自局端末としての機能を実現し、自局端末宛のパケットを振分部７より受け取り、自局端末発のパケットを送信制御部１０に渡し、ユーザインタフェース１より設定されたＶＰＮの設定情報をＳＰ・ＳＡ生成部３に渡す部である。
ＳＰ・ＳＡ生成部３は、ＶＰＮの設定情報、他ＶＰＮ装置と相互通信して受け取った情報を自局制御部２より受け取り、これらの情報からＳＰデータ，ＳＡデータを生成して、ＳＰデータを精査部５に、ＳＡデータの認証鍵を鍵処理部１２に渡し、鍵処理部１２から受け取ったＨＭＡＣ鍵処理後のデータをＳＡデータの一部として、ＳＡデータを振分部７に渡す部である。以下、鍵処理部１２から受け取ったＨＭＡＣ鍵処理後のデータを中間鍵という。ＨＭＡＣ鍵処理については後述する。
【００２１】
受信部４はパケットを受信し、精査部５はＳＰデータのデータベースＡ（ＳＰＤ）６への登録及び受信部４によって受信されたパケットの精査を行う。したがって、データベースＡ（ＳＰＤ）６は、ＳＰデータを保存する。
振分部７は、ＳＡデータをデータベースＢ（ＳＡＤ）８に登録し、自局宛パケットを自局制御部２に、ＩＰＳＥＣ対象外パケットを送信制御部１０に、ＩＰＳＥＣ処理対象パケットを暗号・認証処理部９に、またこのときデータベースＢ（ＳＡＤ）８よりＳＡデータを読み出して暗号・認証処理部９に渡す部である。したがって、データベースＢ（ＳＡＤ）８は、ＳＡデータを保存するデータベースであり、下記に示す鍵処理部が生成した中間鍵を記憶するデータベースの一例である。
暗号・認証処理部９は、パケットのＩＰＳＥＣ処理を行い、パケットに含まれるメッセージを暗号化するとともに上記データベースに記憶した中間鍵を認証鍵として使用して暗号化したメッセージを認証する。
送信制御部１０は自局制御部２、暗号・認証処理部９、振分部７より受け取った送信パケ

ットの宛先を制御し、送信部１１はパケットを送信する部である。
鍵処理部１２はＳＰ・ＳＡ生成部３から受け取った認証鍵のＨＭＡＣ鍵処理を行い、中間鍵を生成して、これをＳＰ・ＳＡ生成部に渡す部である。すなわち、鍵処理部１２は、鍵に関する所定のデータ（ＳＰ・ＳＡ生成部３から受け取った認証鍵）から中間鍵を生成する。
暗号化装置２０は、上記鍵処理部１２と暗号・認証処理部９によって構成され、データベースＢ（ＳＡＤ）８を内部に記憶していても外部に記憶していてもよい。
【００２２】
次に、本実施の形態における発明のＶＰＮ装置３０の処理の流れを図２に添って説明する。パケット処理の前準備として、まずはＳＰデータ、ＳＡデータの登録を行い、その後パケットのＩＰＳＥＣ処理を行う。
【００２３】
まず、ＳＰデータ、ＳＡデータを生成するために、ＶＰＮ管理者がＶＰＮ装置自局端末のユーザインタフェース１を介してＶＰＮ装置３０の設定を行い、自局制御部２はユーザインタフェース１から受け取った情報をＳＰ・ＳＡ生成部３に渡し、ＳＰ・ＳＡ生成部３はＶＰＮ装置３０の設定データであるＳＰデータを生成後（Ｔ１）、これを精査部５に渡し、精査部５はＳＰデータをデータベースＡ（ＳＰＤ）６に登録する（Ｔ２）。
【００２４】
次にＶＰＮ装置間でＶＰＮを構築するため、ＶＰＮ装置間で他のＶＰＮ装置と相互通信を行いＳＡデータを生成する。ＳＰ・ＳＡ生成部３は、ＳＡデータを決定するための他ＶＰＮ装置宛のデータを自局制御部２に渡し、自局制御部２はこれをパケット化して送信制御部１０に渡し、送信制御部１０は送信部１１に渡し、送信部１１はこれを装置外に送信する。
受信部４は他ＶＰＮ装置からのＳＡデータを決定するための情報を持つ受信パケットを精査部５に渡し、精査部５は振分部７に渡し、振分部７は本装置宛と判断し、このパケットをＳＰ・ＳＡ生成部３に渡す。以上の通信によりＳＡデータを生成、決定（Ｔ３）したら、ＳＰ・ＳＡ生成部３はＳＡデータの認証鍵を鍵処理部１２に渡し、鍵処理部１２はＨＭＡＣ鍵処理（図２では鍵（Ｙ１）のハッシュ処理１：Ｔ４，鍵（Ｚ１）のハッシュ処理２：Ｔ５で示す）を行い、これにより得た中間鍵をＳＰ・ＳＡ生成部３に渡す。
ＳＰ・ＳＡ生成部３はＳＡデータを振分部７に渡し、振分部７はこれをデータベースＢ（ＳＡＤ）８に登録する（Ｔ６）。
【００２５】
受信部４は、ＩＰＳＥＣ処理対象パケットを受信し（Ｔ７）、精査部５に渡す。
精査部５は、このパケットはＩＰＳＥＣ処理対象であると判断し、データベースＡ（ＳＰＤ）６よりこのパケットに対応するＳＰＩを読み出し、これとパケットを振分部７に渡す。振分部７はＳＰＩ（ＳＥＣＵＲＩＴＹ　ＰＡＲＡＭＥＴＥＲＳ　ＩＮＤＥＸ）を元にデータベースＢ（ＳＡＤ）８からＳＡデータを読み出し、これとパケットを暗号・認証処理部９に渡す。
暗号・認証処理部９はＳＡデータに含まれる処理情報を元にパケットのＩＰＳＥＣ処理を行い、処理後のパケットを送信制御部１０に渡す。
ここで、ＳＡデータで示された処理が認証処理を含む場合、暗号・認証処理部９はパケットに含まれるメッセージのＨＭＡＣ処理を行う（（図２ではメッセージ（Ｙ２）のハッシュ処理１：Ｔ８、メッセージ（Ｚ２）のハッシュ処理２：Ｔ９で示す）。
送信制御部１０は、暗号・認証処理部９から受け取ったパケットが他ＶＰＮ装置宛であると判断し、これを送信部１１に渡す。送信部１１はパケットを装置の外へ送信する。
【００２６】
次に、図２のＴ４で示す鍵（Ｙ１）のハッシュ処理１（ＨＭＡＣ鍵処理）について図３を用いて説明する。
まず、鍵処理部１２は、認証鍵Ｋに０をパディングし、使用するハッシュ関数のブロックサイズに合わせ、これとｉｐａｄの排他的論理和を行いＩＫ１を生成する（Ｙ０）。

次に、鍵処理部１２は、中間鍵ａであるＭＫ１を生成する。ハッシュ初期値はハッシュ関数ＭＤ５、ハッシュ関数ＳＨＡ１で定義されているハッシュ初期値Ｈ０を用い、被ハッシュデータは上記Ｙ０で生成したＩＫ１を用いて、これらのデータに１ブロックサイズのハッシュ処理を行い、ＭＫ１（中間鍵ａ）を生成する（Ｙ１）。

【００２７】

次に、上記Ｔ５で示す鍵（Ｚ１）のハッシュ処理２（ＨＭＡＣ鍵処理）について図４を用いて説明する。

Ｚ０では、鍵処理部１２は、Ｙ０と同様、認証鍵Ｋに０をパディングし、使用するハッシュ関数のブロックサイズにあわせ、これとｏｐａｄの排他的論理和を行い、ＩＫ２を生成する。

次に、上記鍵（Ｙ１）のハッシュ処理１と同様、鍵処理部１２は、中間鍵ｂであるＭＫ２を生成する。ハッシュ初期値はハッシュ関数ＭＤ５、ＳＨＡ１で定義されているハッシュ初期値Ｈ０を用い、被ハッシュデータをＩＫ２として１ブロックサイズのハッシュ処理を行い、ＭＫ２（中間鍵ｂ）を生成する。

【００２８】

本実施の形態の発明のＶＰＮ装置３０の暗号側におけるデータベースＡ（ＳＰＤ）６とデータベースＢ（ＳＡＤ）８の構造を図５に示す。

ＨＭＡＣ鍵処理において、鍵処理部１２は、Ｙ１の処理後のデータ（ＭＫ１）を中間鍵ａ、鍵（Ｚ１）のハッシュ処理２後のデータ（ＭＫ２）を中間鍵ｂとし、この中間鍵ａ、中間鍵ｂは、振分部７によって認証鍵としてデータベースＢ（ＳＡＤ）８に登録される。中間鍵ａ、中間鍵ｂは、従来の認証鍵の代わりに登録される鍵である。

【００２９】

次に、図２で示されるＴ８の処理について説明する。

図６にメッセージ（Ｙ２）のハッシュ処理１（Ｔ８）で行われる処理を示す。まず、暗号・認証処理部９は、Ｙ２０にてＩＫ１の後ろにＨＭＡＣ処理対象データＰを付加し、さらにパディングデータ　ＰＡＤ　ＤＡＴＡ、データ長Ｌを付加し、ハッシュ関数のブロックサイズの倍数となるハッシュ処理対象データＩＰ１を生成する。

次に、暗号・認証処理部９は、ハッシュ初期値としてＭＫ１（中間鍵ａ）を用い、被ハッシュデータをＩＰ１におけるＩＫ１の後ろの１ブロック分ＩＰ１（１）として１ブロックサイズのハッシュ処理を行いＭＰ１（１）を生成する。次に、ハッシュ処理対象データ分の処理が完了したかどうか判定し（Ｙ２４）、未処理のハッシュ処理対象データがある場合は上述したＹ２２の処理を繰り返し行う。ここでＹ２２におけるハッシュ初期値は前回のＹ２２の結果ＭＰ１（Ｎ－１）とする。

ハッシュ処理対象データ分の処理が完了されたと判断した場合は（Ｙ２４）、最終的に得たＭＰ１（Ｎ）をＤ１として終了する。

【００３０】

次に、図２で示されるＴ９の処理について説明する。

図７にメッセージ（Ｚ２）のハッシュ処理２（Ｔ９）で行われる処理を示す。まず、暗号・認証処理部９は、Ｚ２０にてＩＫ２の後ろにＴ８の結果得られたダイジェストＤ１を付加し、さらにパディングデータＰＡＤ　ＤＡＴＡ、データ長Ｌを追加し、ハッシュ関数の２ブロックサイズになるハッシュ処理対象データＩＰ２を生成する。

次に、暗号・認証処理部９は、Ｚ２２にて、ハッシュ初期値としてＭＫ２（中間鍵ｂ）を用い、被ハッシュデータをＩＰ２（１）として１ブロックサイズのハッシュ処理を行い、この結果をダイジェストＤ２とする。

最終的にダイジェストＤ２の上位９６ｂｉｔがＩＰＳＥＣパケットの認証ダイジェストとして付加される。

【００３１】

以上、暗号化装置２０によってＨＭＡＣ処理によりＩＰＳＥＣ認証処理を行うＶＰＮ装置３０において、認証鍵データに対するハッシュ処理のみを先に実行する鍵処理部１２を設け、ハッシュした結果（中間鍵ａ、中間鍵ｂ）を認証鍵の代わりにデータベースＢ（ＳＡ

Ｄ）８に記憶し、ＨＭＡＣ処理にて繰り返し認証鍵データのハッシュ処理を行う代わりに、データベースＢ（ＳＡＤ）８に記憶してあるハッシュ結果のデータ（中間鍵ａ、中間鍵ｂ）を読み出して使うことにより、ＩＰＳＥＣ認証処理対象パケットごとに実行することが必要であった認証鍵データのハッシュ処理を１回で済むようにすることにより、ＨＭＡＣ処理を高速に行えるようにしたことで、ＩＰＳＥＣ認証処理を高速に行えるようにしたことを特徴とするＶＰＮ装置について説明した。

【００３２】

このように、ＶＰＮ装置３０に含まれる暗号化装置２０は、鍵に関する所定のデータから中間鍵を生成する鍵処理部１２と、鍵処理部１２が生成した中間鍵を記憶するデータベース（データベースＢ（ＳＡＤ）８）と、パケットに含まれるメッセージを暗号化するとともにデータベース（データベースＢ（ＳＡＤ）８）に記憶した中間鍵を認証鍵として使用して、上記中間鍵をハッシュ関数に代入することにより暗号化したメッセージを認証する暗号・認証処理部９とを備えている。

【００３３】

そして、暗号化装置２０は、上記暗号・認証処理部９が認証したメッセージを含むパケットの通信をＩＰＳＥＣプロトコル（ＩＰ　ＳＥＣＵＲＩＴＹ　ＰＲＯＴＯＣＯＬ）に準拠して行うことでＶＰＮ（ＶＩＲＴＵＡＬ　ＰＲＩＶＡＴＥ　ＮＥＴＷＯＲＫ）によるパケット通信を行う。

【００３４】

また、本実施の形態の通信装置（ＶＰＮ装置３０）は、上記暗号化装置２０の鍵処理部１２による中間鍵生成と、鍵処理部１２が生成した中間鍵を記憶するデータベース（データベースＢ（ＳＡＤ）８）と、パケットに含まれるメッセージを暗号化するとともにデータベース（データベースＢ（ＳＡＤ）８）に記憶した中間鍵を認証鍵として使用して暗号化したメッセージを認証する暗号・認証処理部９と、上記暗号・認証処理部９によって認証されたメッセージを含むパケットを送信する送信部１１を備える。

【００３５】

このように構成されたＶＰＮ装置では、ＨＭＡＣ鍵処理については、ＳＡデータ登録時に鍵処理部１２で行われるため、暗号・認証処理部９で行う必要はない。

上述したＨＭＡＣ鍵処理は図２の鍵（Ｙ１）のハッシュ処理１（Ｔ４）及び鍵（Ｚ１）のハッシュ処理２（Ｔ５）に相当し、計２ブロック分の時間を要する。従来の認証鍵の代わりにＨＭＡＣ鍵処理部で生成された中間鍵（中間鍵ａ、中間鍵ｂ）をＳＡデータの一部とし、ＳＰ・ＳＡ生成部３はＳＡデータを振分部７に渡し、振分部７はこれをデータベースＢ（ＳＡＤ）８に登録する。暗号・認証処理部９では、この中間鍵を用いることで１つのパケット認証処理ごとに２ブロック分減らすことができる。

【００３６】

実施の形態２．

実施の形態１では鍵処理部１２を設けているが、図８のようにデータベースＢ（ＳＡＤ）８へのアクセスを振分部７から暗号・認証処理部９に移し、ＳＡデータ登録時に振分部７はＳＡデータを暗号・認証処理部９に渡し、暗号・認証処理部９はＨＭＡＣ鍵処理を行い、その後に暗号・認証処理部は中間鍵を含むＳＡデータをデータベースＢ（ＳＡＤ）８に登録することで、鍵処理部１２を設けずに本発明を実現することも可能である。

【００３７】

このように、本実施の形態では、図８のようにシステムを構成することによって、データベースＢ（ＳＡＤ）８への登録時に認証鍵データに対するハッシュ処理のみを先に実行し、ハッシュした結果（中間鍵ａ、中間鍵ｂ）を認証鍵の代わりにデータベースＢ（ＳＡＤ）８に記憶し、ＨＭＡＣ処理にて繰り返し認証鍵データのハッシュ処理を行う代わりに、データベースＢ（ＳＡＤ）８に記憶してあるハッシュ結果のデータ（中間鍵ａ、中間鍵ｂ）を読み出して使うことにより、ＩＰＳＥＣ認証処理対象パケットごとに実行することが必要であった認証鍵データのハッシュ処理を１回で済むようにすることにより、ＨＭＡＣ処理を高速に行えるようにしたことで、ＩＰＳＥＣ認証処理を高速に行えるＶＰＮ装置を

構築することができる。
【００３８】
このように、本実施の形態のＶＰＮ装置３０に含まれる暗号化装置２０は、鍵に関する情報を記憶するデータベース（データベースＢ（ＳＡＤ）８）と、鍵に関する所定のデータから中間鍵を生成し、生成した中間鍵を上記データベース（データベースＢ（ＳＡＤ）８）に記憶し、パケットに含まれるメッセージを暗号化するとともに上記データベース（データベースＢ（ＳＡＤ）８）に記憶した中間鍵を認証鍵として繰り返し使用してメッセージを認証する暗号・認証処理部９とを備える。
【００３９】
実施の形態３．
他の実施の形態として、暗号・認証処理部９に中間鍵を保存する領域を設けることが考えられる。
本実施の形態を図９に示す。暗号・認証処理部９は中間鍵メモリ１５を内部に持ち、ある認証鍵における最初のパケット認証処理時に中間鍵を中間鍵メモリ１５に保存し、以降同鍵を使用するパケット認証処理時はこの中間鍵を中間鍵メモリ１５より読み出して使用することで実施の形態１、実施の形態２と同等の効果が得られる。
【００４０】
このように、本実施の形態では、図９のようにシステムを構成することによって、認証鍵データに対するハッシュ処理の結果（中間鍵ａ、中間鍵ｂ）を保存する領域（中間鍵メモリ１５）を設け、ある認証鍵での最初のパケット認証時に中間鍵メモリ１５に保存し、以降のパケット認証処理時に中間鍵メモリ１５に保存された中間鍵（中間鍵ａ、中間鍵ｂ）読み出して使うことにより、ＩＰＳＥＣ認証処理対象パケットごとに実行することが必要であった認証鍵データのハッシュ処理を、１回で済むようにすることにより、ＨＭＡＣ処理を高速に行えるようにしたことで、ＩＰＳＥＣ認証処理を高速に行えるようにしたＶＰＮ装置を構築することができる。
【００４１】
このように、本実施の形態のＶＰＮ装置３０に含まれる暗号化装置２０は、鍵に関する所定のデータから中間鍵を生成し、複数のパケットの第１のパケットに含まれるメッセージを暗号化し、生成した中間鍵を使用して暗号化したメッセージを認証するとともに生成した中間鍵を中間鍵メモリ１５に記憶し、上記複数のパケットの第１のパケット以外のパケットに含まれるメッセージを暗号化するとともに中間鍵メモリ１５に記憶した中間鍵を繰り返し使用して認証する暗号・認証処理部９を備える。
【００４２】
上述した全ての実施の形態で得られる効果について説明する。
図１０は、短パケットに対しＩＰＳＥＣ認証処理する場合の、一般的なＶＰＮ装置と上記すべての実施の形態に係る発明のＶＰＮ装置におけるＨＭＡＣ処理時間の比較を図１０に示す。
図１０の通り、あるＳＡデータによる１個目のパケット処理完了までに要する時間は従来の方法とほぼ同じである。しかし２個目以降は各パケットに付き２ブロック分の処理時間短縮となり、Ｎ個処理した場合は２（Ｎ－１）ブロック分の時間短縮となる。図１０は短パケットのときを例としているが、それ以外の長さのパケットを処理した場合も効果は同等である。
【００４３】
上記すべての実施の形態の暗号側のＶＰＮ装置は、復号側のＶＰＮ装置にも適用することができる。復号側のＶＰＮ装置ではＩＰＳＥＣ処理のうち、認証処理手順は暗号側と同じなので、同様の効果が実現可能である。
【００４４】
すなわち、ＩＰＳＥＣ処理の流れとして、暗号化装置の中では暗号処理部の後に認証処理部があり、暗号処理後のデータを認証処理部で認証処理を行う。一方、復号装置の中では認証処理部の後に復号処理部があり、認証処理部で認証処理を行った後で復号処理を行う

。ここで暗号側、復号側の認証処理部は同一のものであるため、復号側においても上記すべての実施の形態の発明による認証処理手順を用いることができ、また、認証処理対象データ、認証鍵についても同一であるため、復号装置でも暗号化装置と同様の効果が実現可能である。

【００４５】

また、上記すべての実施の形態の発明はＨＭＡＣ内で使用される認証アルゴリズムに依存することなく、ＳＨＡ１、ＭＤ５の両方で適用可能であり、また他のブロックサイズの認証アルゴリズムにも適用可能である。

【００４６】

また、上記すべての実施の形態における発明では、通信装置の例としてＶＰＮ装置を挙げているが、ソフトウェアによって実装する場合においても本発明は有効である。

【００４７】

図１１は、上記すべての実施の形態における通信装置のコンピュータ基本構成図である。図１１において、プログラムを実行するＣＰＵ４０は、バス３８を介してモニタ４１、キーボード４２、マウス４３、通信ポート４４、磁気ディスク装置４６等と接続されている。

磁気ディスク装置４６には、ＯＳ４７、プログラム群４９、ファイル群５０が記憶されている。ただし、プログラム群４９、ファイル群５０が一体となってオブジェクト指向のプログラム群４９を形成する形態も一実施の形態として考えられる。

上記鍵処理部１２や上記暗号・認証処理部９等が行う動作は、プログラムとして記述することができる。これらのプログラム群４９が磁気ディスク装置４６に記憶され、ＯＳ４７を使用してＣＰＵ４０により実行されることにより、上記鍵処理部１２や上記暗号・認証処理部９等が行う動作はソフトウェアによって実装することができる。

上記各実施の形態では、通信装置は、通信ポート４４の機能を使用して、他の通信装置と通信を行う。

【００４８】

以上に記載した「登録する」、「記憶する」という用語は、記録媒体に保存することを意味する。

【００４９】

すべての実施の形態では、各構成要素の各動作はお互いに関連しており、各構成要素の動作は、上記に示された動作の関連を考慮しながら、一連の動作として置き換えることができる。そして、このように置き換えることにより、方法の発明の実施形態とすることができる。

また、上記各構成要素の動作を、各構成要素の処理と置き換えることにより、プログラムの実施の形態とすることができる。

また、プログラムを、プログラムを記録したコンピュータ読み取り可能な記録媒体に記憶させることで、プログラムに記録したコンピュータ読み取り可能な記録媒体の実施の形態とすることができる。

【００５０】

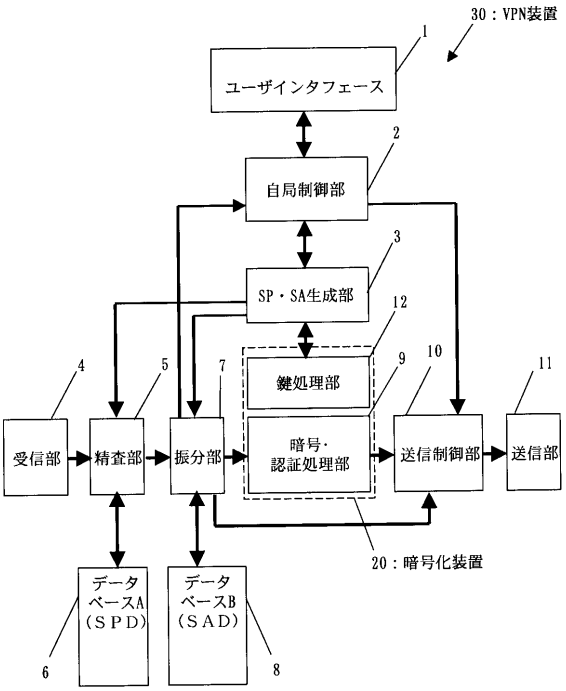
プログラムの実施の形態及びプログラムに記録したコンピュータ読み取り可能な記録媒体の実施の形態は、すべてコンピュータで動作可能なプログラムにより構成することができる。

プログラムの実施の形態およびプログラムを記録したコンピュータ読み取り可能な記録媒体の実施の形態における各処理はプログラムで実行されるが、このプログラムは、記録装置に記録されていて、記録装置から中央処理装置（ＣＰＵ）に読み込まれ、中央処理装置によって、各フローチャートが実行されることになる。

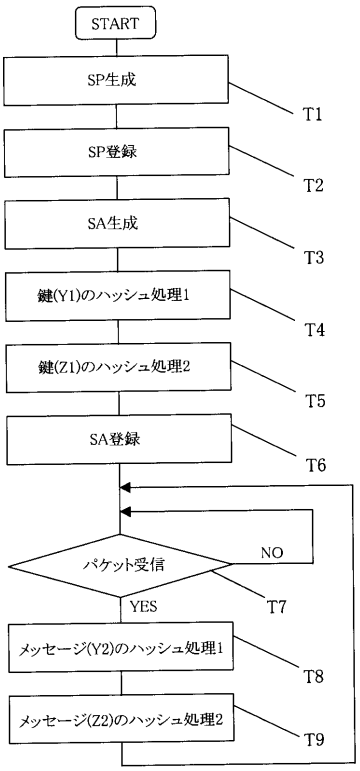
また、各実施の形態のソフトウェアやプログラムは、ＲＯＭ（ＲＥＡＤ　ＯＮＬＹ　ＭＥＭＯＲＹ）に記憶されたファームウェアで実現されていても構わない。あるいは、ソフトウェアとファームウェアとハードウェアとの組み合わせで前述したプログラムの各機能を実現しても構わない。

【００５１】
【発明の効果】
以上のように本発明によれば、ＩＰＳＥＣ認証処理において装置全体の処理時間が短縮され、スループットの向上が測られる。
【図面の簡単な説明】
【図１】本発明の実施の形態１におけるＶＰＮ装置のブロック構成図である。
【図２】本発明の実施の形態１のＶＰＮ装置におけるＩＰＳＥＣ認証処理フローである。
【図３】ＭＫ１（中間鍵ａ）生成フロー図である。
【図４】ＭＫ２（中間鍵ｂ）生成フロー図である。
【図５】各データベースの構造図である。
【図６】ＨＭＡＣ処理の流れを示したフロー図である。
【図７】ＨＭＡＣ処理の流れを示したフロー図である。
【図８】本発明の実施の形態２におけるＶＰＮ装置のブロック構成図である。
【図９】本発明の実施の形態３におけるＶＰＮ装置のブロック構成図である。
【図１０】一般的なＶＰＮ装置とすべての実施の形態に係る発明のＶＰＮ装置におけるＨＭＡＣ処理の効果の差を示した図である。
【図１１】通信装置のコンピュータ基本構成図である。
【符号の説明】
１　ユーザインタフェース、２　自局制御部、３　ＳＰ・ＳＡ生成部、４　受信部、５　精査部、６　データベースＡ（ＳＰＤ）、７　振分部、８　データベースＢ（ＳＡＤ）、９　暗号・認証処理部、１０　送信制御部、１１　送信部、１２　鍵処理部、１５　中間鍵メモリ、３８　バス、４０　ＣＰＵ、４１　モニタ、４２　キーボード、４３　マウス、４４　通信ポート、４６　磁気ディスク装置、４７　ＯＳ、４９　プログラム群、５０　ファイル群。

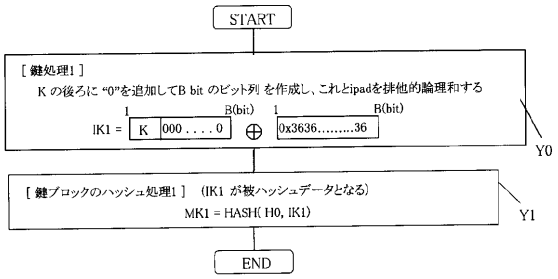
【図１】



【図２】

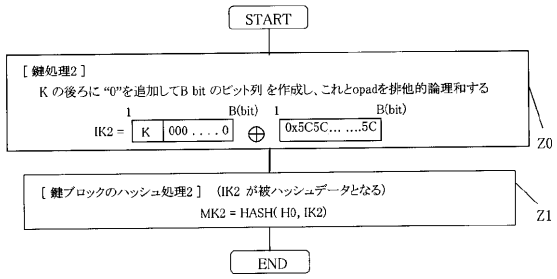


【図３】



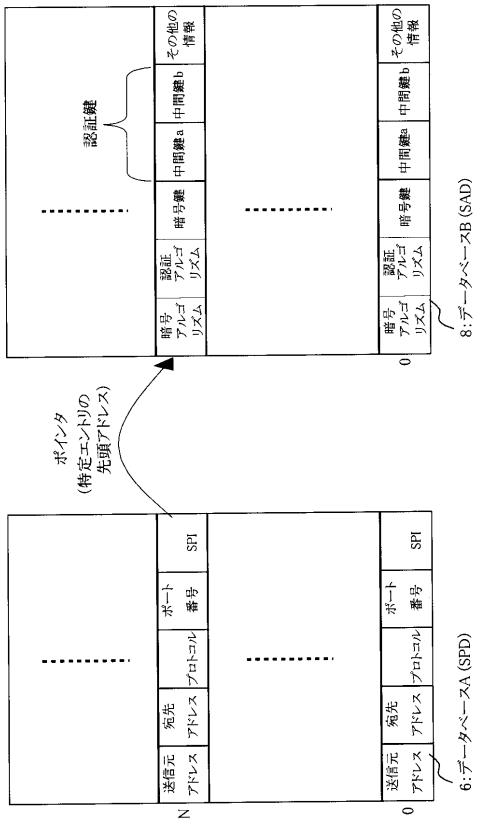
[記号の説明]
HASH(a, b) : ハッシュ初期値 a, 被ハッシュデータ b (B bit) による 1 ブロック単位のハッシュ処理
H0 : MD5, SHA1などで決まっているハッシュ初期値
K : 認証鍵
H : ハッシュ関数
B : Hの 1 ブロックサイズ (H = MD5, SHA1であれば B = 512 bit)
ipad : バイト列 0x36 をB回繰り返したビット列

【図４】

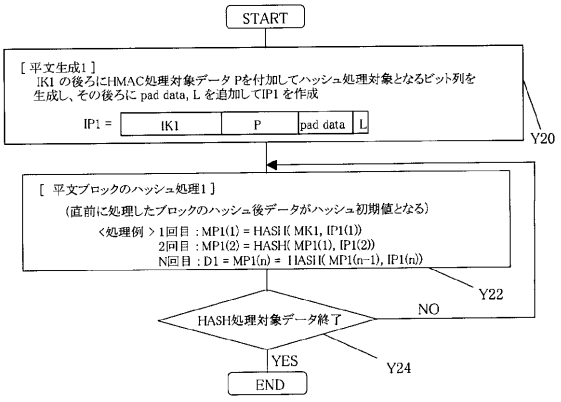


[記号の説明]
opad : バイト列 0x5c をB回繰り返したビット列

【図５】



【図６】

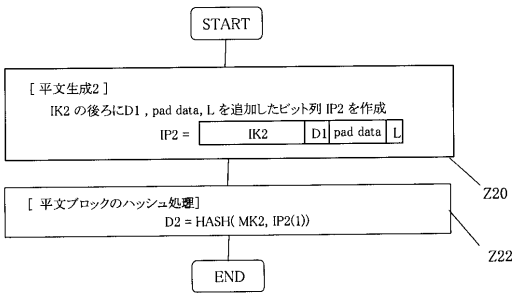


[記号の説明]
pad data : ハッシュ処理するデータ長をブロック境界に合わせるためのパディングデータ
L : ハッシュ処理するデータ長を示す 64bit のビット列
HASH(a, b) : ハッシュ初期値 a, 被ハッシュデータ b (B bit) による 1 ブロック単位のハッシュ処理
H0 : MD5, SHA1などで決まっているハッシュ初期値

ビット列 IP1 の IK1 以下の部分を B bit ずつ区切ったものを IP1(1) IP1(2) …… , IP1(n)
で表す (IP1(*) = 64 byte) 。

IK1(B bit)	IP1(1)	IP1(2)	.....	IP1(n)

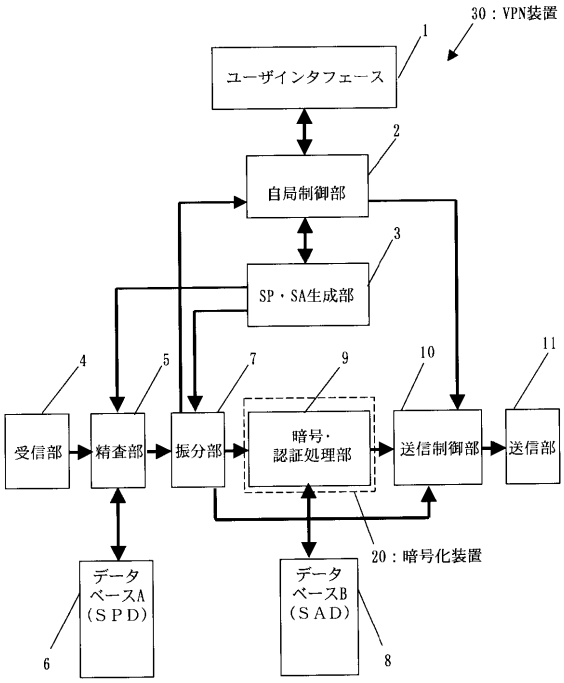
【図７】



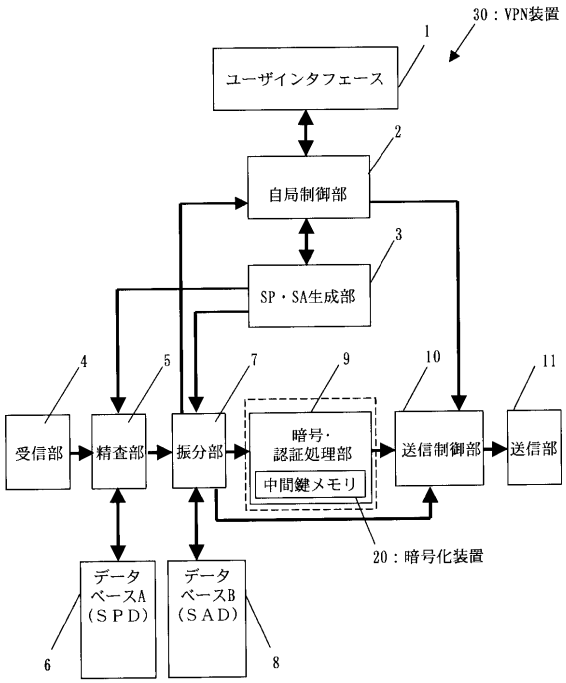
[記号の説明]
ビット列IP2の IK2以下の部分をB bitで区切ったものをIP2(1)で表す。

IK2(B bit)	IP2(1) (B bit)

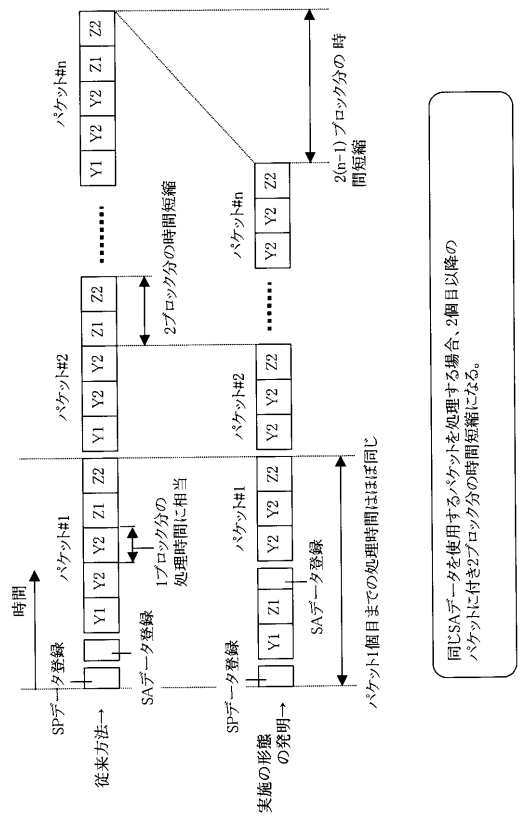
【図８】


30：VPN装置
1
ユーザインタフェース
2
自局制御部
3
SP・SA生成部
4
受信部
5
精査部
7
振分部
9
暗号・
認証処理部
10
送信制御部
11
送信部
20：暗号化装置
データ
ベースA
（SPD）
6
データ
ベースB
（SAD）
8

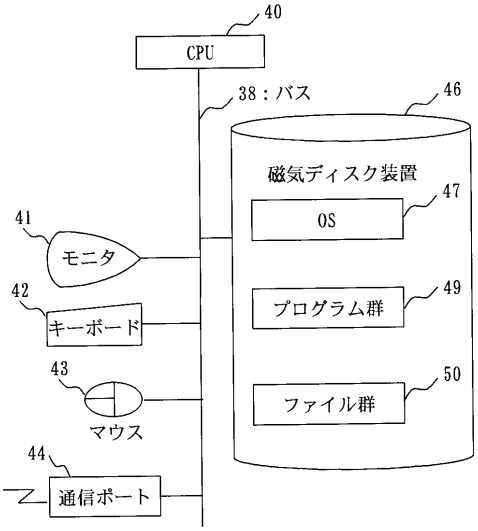
【図９】


30：VPN装置
1
ユーザインタフェース
2
自局制御部
3
SP・SA生成部
4
受信部
5
精査部
7
振分部
9
暗号・
認証処理部
中間鍵メモリ
10
送信制御部
11
送信部
20：暗号化装置
データ
ベースA
（SPD）
6
データ
ベースB
（SAD）
8

【図１０】


時間
SPデータ登録
パケット#1
Y1
Y2
Y2
Z1
Z2
1ブロック分の
処理時間に相当
SAデータ登録
パケット#2
2ブロック分の時間短縮
パケット#n
2(n−1)ブロック分の時間短縮
パケット1個目までの処理時間はほぼ同じ
従来方法→
SPデータ登録
SAデータ登録
実施の形態
の発明→
同じSAデータを使用するパケットを処理する場合、2個目以降の
パケットに付き2ブロック分の時間短縮になる。

【図１１】


40
CPU
38：バス
46
磁気ディスク装置
47
OS
41
モニタ
42
キーボード
49
プログラム群
43
マウス
50
ファイル群
44
通信ポート