参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	SA は、一つ以上のプロポーザルが入った SA ネゴシエーションペイロードである。イニシエータは、ネゴシエーションにあたって複数の提案を**行なってもよい**：レスポンダは一つに対してだけ**リプライしなければならない**。				
	(ISAKMP ヘッダの後に '*' がついて表わされる) メッセージ暗号化は、ISAKMP ヘッダの直後から**始まらなければならない**。通信を保護する場合、ISAKMP ヘッダに続くすべてのペイロードは**暗号化されなければならない**。暗号化鍵は、各アルゴリズム毎に定義される方法にしたがって、SKEYID_e から生成される。				
	メモ中では、Perfect Forward Secrecy (PFS) は、一つの鍵からは、一つの鍵によって保護されたデータだけにしかアクセスを許さないための折り合いという概念を指す。PFS を成り立たせるためには、データの転送を保護するすめに使われる鍵を、更なる鍵の生成に**使ってはならず**、データ転送を保護するために使用される鍵が、別のある鍵素材から生成されたものであるならば、その情報からさらなる鍵を生成してはならない。				
	フェイズ 1 は、二つの ISAKMP ピアが、安全で認証済みの通信するためのチャネルを確立するためのものである。これを ISAKMP SA と呼ぶ。フェイズ 1 交換を確立ものには、「Main モード」と「Aggressive モード」がある。「Main モード」と「Aggressive モード」はフェイズ 1 以外で**使用してはならない**。				
	フェイズ 2 は、鍵素材やパラメータのネゴシエーションを必要とする、IPsec や他のサービスのためのネゴシエーションをするものである。「Quick モード」がフェイズ 2 交換を確立する。「Quick モード」はフェイズ 2 以外で**使用してはならない**。				
	「New Group モード」は、実際フェイズ 1 でもフェイズ 2 でもない。これはフェイズ 1 の次にくるが、先のネゴシエーションで使用されるかもしれない新しいグループを確立するために使用される。「New Group モード」はフェイズ 1 の後以外で**使用してはならない**。				
	SAKMP SA は双方向である。それはつまり、一旦確立されれば、両端のどちらからでも、Quick モード、Informational、New Group モード交換を開始できる。基礎となる ISAKMP ドキュメントによれば、ISAKMP SA は、イニシエータのクッキーとそれに続くレスポンダのクッキーによって区別される。フェイズ 1 交換における両端の役割は、どのクッキーがイニシエータのものかを記録することである。フェイズ 1 交換で確立されたクッキーの並びが、Quick モード、Informational、New Gruop 交換の向きに関係なく、ISAKMP SA を区別する。別の言い方をすれば、ISAKMP SA の向きわ切り替えても、クッキーの順序を**変えてはならない**ということである。				
	本プロトコルでは、自身の DOI を定義しない。フェイズ 1 で確立した ISAKMP SA は、非 ISAKMP サービス (IETF IPSec DOI [Pip97] 等) の DOI と Situation を**使用するかもしれない**このような場合は、実装として、同一 DOI のサービスに対しての SA の確立に、ISAKMP SA の使用を制限することを選択しても**構わない**。反対に、DOI と situation (これらのフィールドについての解説は [MSST98] 参照) の両者の値を 0 として、ISAKMP SA を確立しても**構わない**。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	以下の属性は、IKE で使用され、ISAKMP SA の一部分としてネゴシエーションされる。(これらの属性は ISAKMP SA にだけ関係し、ISAKMP が他のサービスとの関連でネゴシエーションを行なう他の SA とは無関係である。) ＊暗号アルゴリズム ＊ハッシュアルゴリズム ＊認証方法 ＊diffie-Hellman を行なうグループについての情報 これらの属性全ては、必須項目であり、ネゴシエーションされねばならない。それに加えて、オプションで、擬似乱数関数(pseudo-random function:prf) についてのネゴシエーションを行なう事も出来る。(ネゴシエーション可能な擬似乱数関数は、本ドキュメント中では定義されていない。交渉に参加しているものの間で、prf についてのネゴシエーションのために、プライベート使用属性値を使うことができる)。「prf」についてネゴシエーションしなかった場合は、擬似乱数関数として、HMAC ([KBC96] 参照) 版のハッシュアルゴリズムがネゴシエーションされたものとして使用される。他の必須でない属性については、追補Aで解説する。選択されたハッシュアルゴリズムは、ネイティブと HMAC モードの両者をサポートしなければならない。				
	Diffie-Hellman グループは、定義済みのグループ記述 (セクション 6) を使用して指定するか、グループの全ての属性値を定義するか (セクション 5.6) しなければならない。(group タイプや素数など — 追補A 参照) グループ属性は、(予約済みグループ記述や New Group モード交換終了後に確立されるプライベート使用記述のいづれかの) 既に定義されているグループと関連してはならない。				
	IKE 実装は、以下の属性値をサポートしなければならない。 ＊弱いおよびやや弱い鍵チェックの CBC モードの DES [DES] (弱いおよびやや弱い鍵とは、[Sch96] で参照されているもので、追補A に載っている)。その鍵は、追補B にしたがって生成される。 ＊MD5 [MD5] とSHA [SHA] ＊既知共通鍵による認証 ＊デフォルトのグループ番号 0 による MODP (以下を参照) さらに、IKE の実装は、暗号の 3DES、ハッシュの Tiger ([TIGER])、Digital Signature Standard (デジタルサイン標準)、RSA [RSA] サインと RSA 公開鍵暗号を使用する認証、MODP グループ番号 2 をサポートすべきである。IKE の実装は、追補A に定義されている、追加の暗号アルゴリズムのどれをサポートしても構わないし、ECP と EC2N グループをサポートしても構わない。				
	IETF IPsec DOI [Pip97] を実装する際には、ここで解説した IKE モードを実装しなければならない他の DOI でも、ここで解説したモードを使用することがありえる。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	認証された鍵交換を確立するために使用される、二つの基本的な手法 : Main モードとAggressive モードがある。ともに、短時間だけ有効な Diffie-Hellman 交換から、認証された鍵素材を生成する。Main モードは実装しなければならず、Aggressive モードは実装すべきである。さらに、新規の鍵素材を生成し、非 ISAKMP セキュリティサービスをネゴシエーションするためのメカニズムとして、Quick モードは実装されなければならない。また、Diffie-Hellman 交換のプライベートグループを定義するためのメカニズムとして、New Group モードは実装されるべきである。実装は、交換の途中で交換の種類を切り替えてはならない。				
	交換は、標準の ISAKMP ペイロード文法、属性、エンコーディング、タイムアウト、メッセージの再送、を満足しなければならず、例えば、プロポーザルを受け入れられない時や、サイン確認や復号に失敗した時など、通知レスポンスが送られる、Informational メッセージも満足しなければならない、				
	フェイズ 1 交換の間、SA ペイロードは、他の全てのペイロードの前になければならない。特に注記しない限り、メッセージ中の ISAKMP ペイロードの順番には特別な指定はない。				
	フェイズ 1、フェイズ 2 交換に係わらず、KE ペイロードによって渡される Diffie-Hellman 公開値は、ネゴシエーション済みの Diffie-Hellman グループの長さで なければならない。必要な場合は、値 0 を指定する。				
	nonce ペイロードの長さは 8 バイト以上 256 バイト以下でなければならない。				
	同様に、Aggressive モードは、ISAKMP Aggrtessive 交換の具体化である。最初の二つのメッセージでポリシーをネゴシエーションし、Diffie-Hellman 交換値と交換に必要な付随するデータ、ID を交換する。続けて二番目のメッセージでレスポンダを認証する。三番目のメッセージは、イニシエータを認証し、交換への参加の保証を提供する。Aggressive モードの XCHG は、ISAKMP Aggressive である。最後のメッセージは、必要なら、この交換のネゴシエーションが完了するまで、延長することを許している ISAKMP SA による保護を受けない状態で送られることがある。Aggressive モードの図解を見れば、最後のペイロードでは、そうである必要が無いことははっきりわかる。				
	Main モード、Aggresive モード、Quick モードでは、 SA についてのネゴシエーションを行なう。 SA についてのオファーは、 SA ペイロード中に含まれる Proposal ペイロード中に入った Transform ペイロードという形式をとる。フェイズ 1 交換 (MainモードおよびAggressiveモード) で複数のオファーが行なわれる場合、一個の SA ペイロード中の一個の Proposal ペイロードに 複数の Transform ペイロードが入る形式を取らなければならない。他の形式を取るなら、一個の SA ペイロード中に複数の Proposal ペイロードがあってはならず、同時に複数の SA ペイロードが存在する事も許されない。本ドキュメントでは、フェイズ 2 のオファーにおけるその様な行動を禁止していない。				
	イニシエータがレスポンダへ送るオファーの数に制限はないが、仕様を満たす実装では、性能上の問題を考慮して、オファーの数を制限してもかまわない。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	SA ネゴシエーションの間、イニシエータはレスポンダに対し、これから確立する SA についてオファーする。レスポンダは、いかなるオファーについても、例外の属性エンコーディングを除いて、その属性を変更してはならない（追補A参照）。交換のイニシエータが、オファーの属性値が変更されたり、追加/削除されたりしていることに気付いた場合は、そのレスポンスは拒絶しなければならない。				
	使用されているハッシュアルゴリズムは既知であるから、それの OID を署名の中にエンコードする必要はない。付け加えると、本ドキュメント中で使われている PKCS#1 の RSA 署名などの OID に対するバインディングは存在しない。それゆえ、RAS 署名は、（ハッシュアルゴリズムの OID を含む）PKCS#1 形式の署名ではなく、PKCS#1 形式のプライベートキー暗号としてエンコードされなければならない。DSS 署名は、r に s が続くようにエンコードしなければならない。				
	オプションとして、一個以上の証明書ペイロードを**渡してもよい**。				
	公開鍵暗号を使用するためには、イニシエータはレスポンダの公開鍵を持っている必要がある。				
	認証の公開鍵暗号手法を使うことによって、（セクション 5.2 参照）、レスポンダが利用可能な公開鍵を含む複数の証明書を持つ場合、証明書を確認するために HASH ペイロードが送られることがある（例、証明書の制限やアルゴリズムの制限のために、証明書が署名だけのためのものでない場合）。HASH ペイロードが送られる場合、それは二番目のメッセージ交換の一番目のペイロードで、かつそれには暗号化された nonce が続かなければならない。HASHペイロードか送られない時は、二番目のメッセージ交換の最初のペイロードは、暗号化された nonce で なければならない。さらに、イニシエータは、オプションとして、返答するための公開鍵をレスポンダに渡すために 証明書ペイロードを送ってもよい。				
	簡潔にするために、Ke_i の生成についてだけ示した。Ke_r についても同じである。K1 の計算での値 0 の長さは 1 オクテットである。Ne_i、Ne_r、Ke_i、Ke_r はすべてその場限りのもので、使用後廃棄しなければならない。				
	オプションの HASH ペイロードと必須の nonce ペイロードの位置についての要求事項を保持すれば、それ以外にペイロードついて要求されることはない。暗号化された nonce に続くすべてのペイロードは、— いかなる順序であっても — 方向に応じて Ke_i または Ke_r で暗号化されなければならない。				
	Quick モードによって、交換そのものが完了するわけではないが（それはフェイズ 1 交換の役目である）、鍵素材を生成し、非 ISAKMP SA での共有ポリシーをネゴシエーションするために、SA ネゴシエーション処理の一部（フェイズ 2）で使用される。Quick モードで交換される情報は、ISAKMP SA によって保護されなければならない — つまり、ISAKMP ヘッダを除くすべてのペイロードは暗号化されなければならない。Quick モードでは、HASH ペイロードは、ISAKMP ヘッダの直後に、SA ペイロードは HASH ペイロードの直後になければならない。HASH は、メッセージを認証し、同時に生存確認も行なう。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	Quick モードは、基本的に SA ネゴシエーションであり、リプレイ攻撃からの保護を提供するための nonce の交換である。nonce は新しい鍵素材の生成と、でたらめの SA を生成してのリプレイ攻撃を防ぐために使用される。Quick モードにさらなる Diffie-Hellman 交換と指数関数を加えるために、オプションの鍵交換ペイロードを使用できる。Quick モードで鍵交換ペイロードはオプションであるが、サポートしなければならない。				
	Quick モードでネゴシエーションされる SA の ID として、ISAKMP の相手の IP アドレスが仮定される。Quick モードでクライアント ID を指定した場合を除いて、プロトコルやポート番号に対しての制約は許されない。ISAKMP が、一方のクライアント・ネゴシエータである場合、両端の ID は、IDci と IDcr として渡さなくてはならない。指定された ID に対しての提案を受けてるかどうかは、ローカルポリシーが指示する。Quick モード・レスポンダが、(ポリシーや他の理由のために) クライアント ID を受け取らない場合、INVALID-ID-INFORMATION (18) という種類の Notify メッセージが入った Notify ペイロードを送らなければならない。				
	Quick モードの間に行なわれたすべての提案は、論理的に関係しており、食い違いが有ってはならない。例を挙げれば、KE ペイロードを送る場合、Diffie-Hellman グループについて記述する属性 (セクション 6.1 と [Pip97] を参照) に、ネゴシエーション中のすべての SA のすべての提案のすべての変換を含まなければならない。同様に、クライアント ID を使用する場合、ネゴシエーション中のすべての SA にたいして適用しなければならない。				
	(PFS があるにしろないにしろ、直接生成されたものであっても、つなぎあわせたものであっても) この鍵素材は、ネゴシエーションした SA においてのみ使わなければならない。鍵素材からどのようにかぎを生成するかはサービスの責任である。				
	ISAKMP SA が確立されるよりも前に、New Group モードを使用してはならない。新しいグループについての記述は、フェイズ 1 ネゴシエーション以外の後にあってはならない (であるが、フェイズ 2 交換ではない)。				
	プロポーザルによってグループの特性を指定する (追補 A 参照)。プライベートグループについてのグループ記述は、2^15 以上でなければならない。グループを受け入れられない場合、レスポンダは ATTRIBUTE-NOT-SUPPORTED (13) のメッセージ種類の Notify ペイロードで返答しなければならない。				
	ISAKMP の実装は、確立した SA の有効期限を限るために、プライベートグループを要求してもよい。				
	先に注意したように、prf 計算で使用される ISAKMMP ヘッダ中のメッセージ ID は、交換ごとにユニークであり、この Informational 交換を行なわせるフェイズ 2 交換のどれとも同じであってはならない。このメッセージを暗号化するための SKEYID_e で使用される初期配列の生成については、追補 B で説明している。				
	Oakley の実装においては、以下の素数とジェネレータを持つ MODP グループを**サポートしなければならない**。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	IKE の実装においては、以下の素数とジェネレータを持つ MODP グループを**サポートするべきである**。				
	IKE の実装においては、以下の特性を持つ EC2N グループを**サポートするべきである**。				
	IKE の実装においては、以下の特性を持つ EC2N グループを**サポートするべきである**。				
	次は両端の間での最初の交換でのペイロードを図示したものである。イニシエータは複数のプロポーザルを提案してもよい。レスポンダは 1つに対してしか返答してはならない。				
	鍵素材と ID 両方に対しての PFS は、本プロトコルによって達成できる。KE ペイロードで、Diffie-Hellman グループを指定し公開値を渡すことで、ISAKMP 両端は鍵の PFS を確立でき、ID は ISAKMP SA の SKEYID_e によって保護され、それゆえ PFS によっては保護されない。鍵素材と ID 両方に対しての PFS を望む場合は、ISAKMP 端は、(IPsec SA などの) 非ISAKMP SA を ISAKMP SA ごとに一つだけ確立しなければならない。				
	IKE 交換は、使用中の初期化配列 (Initialization vectors:IV) を管理する。最後のメッセージの最後の暗号文ブロックが次のメッセージの IV となる。交換の同期をずらすことになる再送 (もしくは正しいクッキーをもつ偽のメッセージ) を防ぐために、IKE の実装は、複合化したメッセージが基本的な正当性チェックをパスし、IKE ステートマシンが進む先を実際に決定する — これは再送ではない、まで 現行の IV を更新してはならない。				
	属性割り当て番号 フェイズ 1 の間にネゴシエーションされる属性は、以下の定義によっている。フェイズ 2 属性は、DOI 仕様書の中で定義される (例えば、IPsec 属性は IPsec DOI の中で定義される)。が、Quick モードに短時間有効な Diffie-Hellman 交換が含まれる時のグループ記述子は例外である。属性タイプは、基本 (B) もしくは可変長 (V) のいづれかである。これらの属性のエンコーディングは、基礎となる ISAKMP 仕様書の中で、タイプ/値 (基本) とタイプ/長さ/値 (可変長) として定義されている。 基本として解説されている属性を、可変長でエンコードしてはならない。可変長属性は、その長さが 2 オクテットに入るなら、基本属性としてエンコードして構わない。この場合、本プロトコルのイニシエータから可変長 (もしくは基本) として送られてきた属性が、基本 (もしくは可変長) としてイニシエータに返されることがありうる。				

参照資料	管理策	セキュアネットワーク基盤の運用			利用
		ルータのセキュリティ機能	ルータの製造・出荷に係る運用ルール	その他	
	クラス値 鍵長 可変長鍵を持つ暗号アルゴリズムを使用する際に、鍵の長さをこの属性でビット単位で指定する。(ネットワークバイトオーダを使用しなければならない)。指定した暗号アルゴリズムが固定長鍵を使用する場合には、この属性を指定してはならない。				
	この追保では、ISAKMP メッセージを暗号化するさいにだけ使われる、暗号の詳細を解説する。(IPSEC 変換のような) サービスが、鍵素材を発生させるために ISAKMP を利用する場合、すべての暗号アルゴリズム特有の詳細 (鍵、IV 生成、パディング、などなど) は、そのサービスによって定義されなければならない。ISAKMP は、どんな暗号アルゴリズムにも適切な鍵を生成するとは主張していない。ISAKMP は、サービスがそれから適切な鍵を生成しなくてはならない鍵素材を要求された量だけ生成する。鍵の弱さのチェックなどの詳細な点は、サービスの責任である。				
	フェイズ 1 では、CBC モード暗号アルゴリズムの初期化配列のための素材 (IV 素材) は、イニシエータの公開 Diffie-Hellman 値と、レスポンダの公開 Diffie-Hellman 値を結合したものにネゴシエーションの結果のハッシュアルゴリズムを適用した結果から生成したものである。これは最初のメッセージでのみ使用される。各メッセージは、値 0x00 のバイトで一番近いブロックの大きさまでパディングされる。ヘッダ中のメッセージ長は、暗号文の大きさを反映するので、パディングの長さを含まなければならない。続くメッセージは、直前のメッセージを初期化配列として使用しなければならない。				
	RC5-R16-B64-CBC の鍵は、必要な場合は前述の擬似関数乱数フィードバック手法を用いて生成される鍵のネゴシエーションされた大きさか、(ネゴシエーションされなかった時は) 最初の 16 バイトである。IV は上記のように生成された IV 素材の最初の 8 バイトである。ラウンド数は 16 でなければならず、ブロック長は 64 でなければならない。				