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	
	ISAKMPでは、全てのDOIは、"Assigned Number" RFC [STD-2] にある、IANAに登録されなければならない。				
	SIT_IDENTITY_ONLY は、関連する Identification Payload 中にある発信元ID情報によって、SA を確認することを指定する。				
	少なくともフェイズ1 Oakley 交換 ([IKE], セクション5) の Identification Payload の一つを含むようにすることによって、全てのIPSEC DOIの実装は、IT_IDENTITY_ONLYをサポートしなければならず、さらに Identification Payload を含まないすべてのアソシエーション確立を中断しなければならない。				
	イニシエータ(発呼側)が、SIT_SECRECY と SIT_INTEGRITY をともにサポートしない場合、Situation は、4オクテットちょうどの Situation ビットマップだけからなり、Labeled Domain IDフィールド (図1、セクション4.6.1) やそれに続くラベル情報を含まない。逆に、イニシエータが SIT_SECRECY か SIT_INTEGRIRY をサポートする場合は、Labeled Domain IDが Situation Payload に含まれなければならない。				
	SIT_SECRECY は、ネゴシエーション中の SA が、ラベル付けされたセキュリティが必要な環境中にあることを示している。Situation ビットマップ中に SIT_SECRECY があった場合、Situation フィールドには、センシティブティレベルとコンパートメントビットマスクが入った可変長のデータが続く。				
	イニシエータが SIT_SECRECY をサポートしない場合、SIT_SECRECY は Situtaion ビットマップ中に**設定されてはならず**、また秘密レベルやカテゴリビットマップも含まれないほうがよい。				
	レスポンダが SIT_SECRECY をサポートしない場合は、SITUATION-NOT-SUPPORTED 通知ペイロードを**返すべきであり**、SA の確立は**中止されなければならない**。				
	SIT_INTEGRITY は、ネゴシエーション中のSA が、ラベルが付いたインテグリティを必要とする環境中にあることを示している。Situation ビットマップ中に SIT_INTEGRITY があった場合、Situation フィールドには、インテグリティレベルとコンパートメントビットマスクが入った、可変長のデータが続く。				
	イニシエータが SIT_INTEGRITY をサポートしない場合、SIT_INTEGRIRY は Situtaion ビットマップ中に**設定されてはならず**、またインテグリティレベルやカテゴリビットマップも含まれないほうがよい。				
	レスポンダが SIT_INTEGRIRY をサポートしない場合は、SITUATION-NOT-SUPPORTED 通知ペイロードを**返すべきであり**、SA の確立は**中止されなければならない**。				
	使用するOSとインストールされるユーティリティソフトによって変わるが、固定鍵をTCP/IPカーネルに渡してしまうと、もう保護することが出来ないということもあるだろう。だが、システムの起動時に、さらなる認証なしで簡単に再生できるようなことがあってはならない。				

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	
	一晩でIPSECへの移行が済むと考えるのは現実的ではない。ホストシステムが どのシステムと安全に話す必要があり、どのシステムから安全に話される必要があるを記載した、融通のきくポリシーリストを用意しなければならない。プロキシ ファイアウォールのアドレスについての注意書きも必要だろう。				
	最小限、IPアドレス、ネットマスク、安全が必要かどうかのフラグについて確定したリストが必要だろう。				
	より融通が利く実装のためには、ワイルドカードを使ったDNS名 (例、'*.foo.bar')、 入/出のビットマスク、さらに必要ならファイアウォールのアドレスが 載ったリストが必要だ。				
	ワイルドカードDNS名は、入/出のIPアドレスと一致させるために、ビットマスクはセキュリティを確保するかどうかとその方向を決めるために使われ、オ プションのファイアウォールのアドレスは、中継ファイアウォールを通して対象システムとの接続するための、トンネルモードが必要がどうかを示す。				
	証明書を使った認証方式を実装するホストシステムには、証明書の取得、それのデータベースを管理する機構が必要になる。				
	セキュアDNSは証明書配送機構の一つであるが、短期的には、セキュアDNSを使用できるゾーンの広まりが期待できそうにない、さまざまな理由がある。 一番の理由は、ホストが安全な手段で証明書を手に入れる能力が必要になるだけでなく、他のシステムが使う自身の証明書を送り出せなければならないからだ。				
	動的な証明書発見機構やプロトコルが使用可能となった時に、その導入を阻むことになるため、手作業による証明書管理は行なうべきではない。				
	PROTO_ISAKMP波、ISAKMPプロトコルのフェイズ1の間、メッセージを保護する必要があることを示す。IPSEC DOI で使われる、ある保護メカニズムについては、[IKE]で解説されている。全ての IPSEC DOI の実装は、PROTO_ISAKMP を**サポートしなくてはならない**。				
	PROTO_IPSEC_AH は、IPパケット認証を指定する。デフォルトのAH変換は、データ発信元による認証、完全性保護、replay検出を行なう。 輸出制限を考慮する場合、PROTO_IPSEC_AH 変換による秘匿性の提供は**行なってはならない**。				
	PROTO_IPSEC_ESP は、IPパケットの秘匿性を指定する。認証が必要な場合は、それはESP変換の中で提供されなければならない。デフォルトのESP変換には、データ発信元認証、完全性保護、replay生検出、秘匿性が含まれる。				
	KEY_IKEは、[IKE] ドキュメントに定義されている、ハイブリッド ISAKMP/Oakley Diffie-Hellman 鍵交換 (IKE) を指定する。IPSEC DOI のすべての実装は、KEY_IKE を**サポートしなければならない**。				
	正しいAH保護スートを見つけるために、認証アルゴリズム (Authentication Algorithm) 属性を**指定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	
	続くセクションでは、すべての実装義務のあるアルゴリズムについては、実装「しなければならない」(例、AH_MD5)となっている。それ以外のアルゴリズムの実装はオプションであり、実装してもかまわない。				
	IPSEC DOI のすべての実装は、Auth(HMAC-MD5) 属性でのAH_MD5を**サポートしなければならない**。このスートは、[HMACMD5]で、HMAC-MD5-96変換として定義されている。				
	IPSEC DOI のすべての実装は、Auth (HMAC-SHA) 属性での AH_SHA を**サポートしなければならない**。このスートは、[HMACSHA]で、HMAC-SHA-1-96変換として定義されている。				
	認証時、完全性保護、replay生検出は必要であり、適切なESP保護スートを特定できるよう、認証アルゴリズム属性を**指定しなければならない**。例を挙げれば、HMAC-MD5認証を3DESと共に使用したいならば、ESP_3DES変換IDを、HMAC-MD5に設定された認証アルゴリズム属性と共に指定する。				
	IPSEC DOIのすべての実装は、Auth (HMAC-MD5) 属性でのESP_DESを**サポートしなければならない**。				
	IPSEC DOIのすべての実装は、Auth (HMAC-MD5) 属性でのESP_3DESをサポートする様、**強く要請されている**。				
	IPSEC DOIのすべての実装は、ESP_NULLを**サポートしなければならない**。				
	基本となっている属性を**可変長エンコーディングしてはならない**。可変長属性が2オクテットに収まるなら、**基本属性エンコーディングしてもよい**。				
	SA Life Duration 属性は、必ず期間の単位を示す SA Life Type の後に**続かなくてはならない**。				
	認証アルゴリズムにはデフォルト値は存在しないので、以下の例を除いて、使用するAH/ESP変換が正しく判断できるように、アルゴリズムを指定しなくてはならない。				
	ESPで認証無しでネゴシエーションする場合、プロポーザルの中に認証アルゴリズム属性は**あってはならない**。				
	ESPで秘匿性無しでネゴシエーションする場合、プロポーザルの中に認証アルゴリズム属性は**なくてはならず**、ESP変換IDはESP_NULLでなければならない。				
	鍵長にはデフォルトの値は存在しないので、鍵長が可変の暗号を使う変換に対しては、指定しなければならない。固定長の暗号に対して、鍵長属性を**送ってはならない**。				
	鍵ラウンドにはデフォルトの値は存在しないので、ラウンド数が変わる暗号を使う変換に対しては、指定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	
	基本相互運用性を確実にするために、すべての実装では以下の属性全てに対してのネゴシエーションを行えるように**なっていなければならない**。 ＊ SA Life Type ＊ SA Duration ＊ Auth Algorithm				
	セマンティックスの自由度を高めるために、IPSEC DOIは、ISAKMP を満足する実装は属性リストに、ある属性クラスのインスタンスが複数含まれていても、それらが衝突しない限り、正しくパース**できなければならない**ことを要求する。現時点では、この扱いを必要とする属性は、Life TypeとDuration だけである。				
	属性の衝突が見つかったら、ATTRIBUTES-NOT-SUPPORTED Notification ペイロードを**送るべき**であり、SAの確立は**中断されなければならない**。				
	実装は、定義されているがサポートしていないIPSEC DOI属性(もしくは属性値)を受け取った場合、その値が予約されている範囲に入っていないなら、ATTRIBUTES-NOT-SUPPORTED を**送るべき**であり、SAの確立は**中断されなければならない**。				
	実装が予約範囲の属性値を受け取った場合、継続するかどうかを、ローカルポリシーに基づいて**決めて良い**。				
	イニシエータから、レスポンダが受け入れるものよりも長い有効期間が提案された場合、レスポンダは、ISAKMP通知ペイロードを、レスポンダからのIPSEC SAペイロードの交換の中に含めなければならない。この場合に使わなければならない、RESPONDER-LIFETIME通知メッセージは セクション 4.6.3.1で定義されている。				

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	
	SAペイロードの定義は以下の通りである。 ＊ Next Payload (1オクテット) – 同じメッセージ中の次のペイロードの種類のIDである。このペイロードがメッセージ中の最後のものである場合、値は0となる。 ＊ RESERVED (1オクテット) – 未使用。0でなければならない。 ＊ Payload Length/ペイロード長 (2オクテット) – このペイロードの、ヘッダも含んだオクテット単位での長さ。 ＊ Domain of Interpretation/解釈ドメイン (4オクテット) – IPSEC DOI を指定し、その値は1である。 ＊ Situation/状況 (4オクテット) – 残りのSAペイロードを解釈するために使用される ビットマップ。その値すべての一覧については、セクション4.2を参照。 ＊ Labled Domain Identifier/ラベル付きドメインID (4オクテット) – Secrecy/秘匿性とIntegrity/完全性の解釈に使われるIANA割当番号。 ＊ Secrecy Length/秘匿性長 (2オクテット) – パッディングビットを除いて、秘匿性レベルIDの長さを、オクテット単位で指定する。 ＊ RESERVED (2オクテット) – 未使用。0でなければならない。 ＊ Secrecy Level/秘匿性レベル (可変長) – 要求される必須秘匿性レベルを指定する。 秘匿性レベルは、32ビット境界に並ぶように、0でパディングされなければならない。				
	＊ Secrecy Category Length/秘匿性カテゴリ長 (2オクテット) – パディングビットを除いた、秘匿性カテゴリ(コンパートメント)ビットマップの長さを、ビット単位で指定する。 ＊ RESERVED (2オクテット) – 未使用。0でなければならない。 ＊ Secrecy Category Bitmap/秘匿性カテゴリビットマップ (可変長) – 要求される秘匿性カテゴリ(コンパートメント)を示すために使用される ビットマップ。ビットマップは、32ビット境界に並ぶように、0でパディングされなければならない。 ＊ Integrity Level/完全性レベル (2オクテット) – パディングビットを除いた、完全性レベルIDの長さを、オクテット単位で指定する。 ＊ RESERVED (2オクテット) – 未使用。0でなければならない。 ＊ Integrity Level/完全性レベル (2オクテット) – 要求される必須完全性レベルを指定する。完全性レベルは、32ビット境界に並ぶように、0でパディングされなければならない。 ＊ Integrity Category Length/完全性カテゴリ長 (2オクテット) – パディングビットを除いた、完全性カテゴリ(コンパートメント)ビットマップの長さを、ビット単位で指定する。 ＊ RESERVED (2オクテット) – 未使用。0でなければならない。 ＊ Integrity Category Bitmap/完全性カテゴリビットマップ (可変長) – 要求される完全性カテゴリ(コンパートメント)を示すために使われるビットマップ。ビットマップは、32ビット境界に並ぶように、0でパディングされなければならない。				

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	
	IDペイロードは、SAのイニシエータのイニシエータが本物である事を確認するために使用される。レスポンダは、アソシエーションに必要な 正しいホストシステムセキュリティポリシーを決定するために、イニシエータのIDを**使用すべきである**。				
	フェイズIネゴシエーション中、IDポートとプロトコルフィールドは0か、UDPポート500で**なければならない**。実装が他の値を受け取った時は、エラーと**しなければならず**、SAの確立は、**中断しなければならない**。このイベントは**記録されるべきである**。				
	IDペイロードの各フィールドは以下のように定義されている。 ＊ Next Payload (1オクテット) - 同じメッセージ中の次のペイロードの種類のIDである。このペイロードがメッセージ中の最後のものである場合、値は0となる。 ＊ RESERVED (1オクテット) - 未使用。0でなければならない。 ＊ Payload Length/ペイロード長 (2オクテット) - このペイロードの、ヘッダも含んだオクテット単位での長さ。 ＊ IDタイプ (1オクテット) - Identification Data(ID)フィールドにある情報の種類を決める値。 ＊ Protocol ID/プロトコルID - 対応するIPのプロトコルID (例、UDP/TCP) を指定する値。 値が0の場合は、Protocol IDフィールドを無視しなければならない。 ＊ Port/ポート (2オクテット) - 対応するポート番号を指定する値。値が0の場合は、Portフィールドを無視しなければならない。 ＊ Identification Data/IDデータ (可変長) - Identification Type で指定される値。				
	(なんらかの)証明書を使ってIKE交換を認証する場合、ポリシーに基づく決定に使用されるIDはすべて、交換の認証に使われる証明書のなかに**入っているべき**である。				
	ID_FQDNは、省略無しのドメイン名(FQDN)文字列を示す。"foo.bar.com" が ID_FQDN の例である。文字列には、終端文字を含むべきではない。				
	ID_USER_FQDNは、省略無しのユーザ名文字列を示す。"piper@foo.bar.com" がID_USER_FQDNの例である。文字列には、終端文字を含むべきではない。				
	Aggressiveモードでは、交換と状態通知メッセージをバインドするために必要な 保護が提供されないので、状態通知メッセージは、最後のMainモード交換のペイロード、もしくは、MainモードまたはAggressiveモード処理 の完了後の独立したInformational交換、またはQuickモード交換のペイロードとして、ISAKMP SA の保護のもので**送られなければならない**。				

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	
	ISAKMPプロトコルは、KSAKMP Informational 交換で起こられた場合、状態通知メッセージが配送される事を保証しない。メッセージが受信される事を確実にするには、再送タイマーで保護される、Mainモードか Quick モード交換に通知ペイロードを**入れるべきである**。				
	使用された場合、通知ペイロードの形式は以下の通りで**なければならない**。 ＊ Payload Length – ペイロード長+データ長(可変) ＊ DOI – IPSEC DOI (1)に設定 ＊ Protocol/プロトコル ID – 選んだSAのプロトコルIDに設定 ＊ SPIサイズ – 16(2個の8オクテットISAKMPクッキー)もしくは4(IPSEC SPI一個) ＊ Notification Message Type/通知メッセージタイプ – RESPONDER-LIFETIME(セクション4.6.3)に設定 ＊ SPI – 二個のISAKMPクッキーもしくは送信元の受信IPSEC SPI ＊ Notification Data/通知データ – レスポンダの実際のSA有効期間のISAKMP属性リスト				
	使われた時は、Notification Payload/通知ペイロードは以下の形式で**なければならない**。 ＊ Payload Length – ペイロード長+データ長(4) ＊ DOI – IPSEC DOI (1)に設定 ＊ Protocol/プロトコル ID – 選んだSAのプロトコルIDに設定 ＊ SPIサイズ – 16(2個の8オクテットISAKMPクッキー)もしくは4(IPSEC SPI一個) ＊ Notification Message Type/通知メッセージタイプ – REPLAY-STATUSに設定 ＊ SPI – 二個のISAKMPクッキーもしくは送信元の受信用IPSEC SPI ＊ Notification Data/通知データ – 4オクテットの値: o 0 = 再送検出非動作 o 1 = 再送検出動作				
	INITIAL-CONTACT状態メッセージは、片側から他方へ、そことSAを確立するのが始めてである事を通知したい場合に使用される。この通知メッ セージの受信側は、送信元が再起動したため、以前のSAとそのに関係する鍵情報にはアクセスできなくなったのだろうとみなして、そのシステムに対しての既 存のSAを削除することができる。これが使われる場合、通知データフィールドの内容は空 (null) で**あるべきである** (つまり Payload Length を通知ペイロードのある固定長になるはずである)。				

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	
	あった場合は、通知ペイロードは以下の形式に**なっていなければならない**。 ＊ Payload Length – ペイロード長+データ長(0) ＊ DOI – IPSEC DOI(1)に設定 ＊ Protool ID – 選択したSAから選ばれた Protocol ID に設定 ＊ SPI Size – 16(二つの8オクテットISAKMPクッキー) ＊ Notify Message Type – INITIAL-CONTACT に設定 ＊ SPI – 2個のISAKMPクッキーに設定 Notification Data – なし				
	Situation Definition は、IPSEC SA 申し込みとネゴシエーションが動作する環境を表現する、32ビットのビットマスクである。新しいSituationの割当の要求は、割り当てられるビットの解釈を解説するRFCによらなければならない。				
	標準化目的でない（つまり、Informatial/広報やexperimental/実験）RFCであるなら、RFCを出し変換IDが割り当てられる前に、IESGによって明確にレビューされ承認されなければならない。				
	セキュリティプロトコルIDは、ネゴシエーションするセキュリティプロトコルスートを表わす、8ビットの値である。新セキュリティプロトコルIDの割当の要求は、要求するセキュリティプロトコルを解説するRFCによらなければならない。[AH] と [ESP] はセキュリティプロトコルドキュメントの例である。				
	標準化目的でない（つまり、Informatial/広報やexperimental/実験）RFCであるなら、RFCを出し変換IDが割り当てられる前に、IESGによって明確にレビューされ承認されなければならない。				
	IPSEC ISAKMP 変換ID は、ネゴシエーションで使われる鍵交換プロトコルを表わす8ビットの値である。新ISAKMP変換IDの割当の要求は、要求する鍵交換プロトコルを解説するRFCによらなければならない。				
	標準化目的でない（つまり、Informatial/広報やexperimental/実験）RFCであるなら、RFCを出し変換IDが割り当てられる前に、IESGによって明確にレビューされ承認されなければならない。				
	IPSEC AH 変換IDは、AHに対して完全性保護を提供するために使われる、ある一つのアルゴリズムを表わす8ビットの値である。新 AH 変換 ID の割当の要求は、AHフレームワーク（[AH]）内でのアルゴリズムの使用方法を解説するRFCによらなければならない。				
	標準化目的でない（つまり、Informatial/広報やexperimental/実験）RFCであるなら、RFCを出し変換IDが割り当てられる前に、IESGによって明確にレビューされ承認されなければならない。				
	IPSEC ESP変換IDは、ESPに対してセキュリティ保護を提供するために使われる、ある一つのアルゴリズムを表わす8ビットの値である。新ESP変換IDの割当の要求は、ESPフレームワーク（[ESP]）内でのアルゴリズムの使用方法を解説するRFCによらなければならない。				

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	
	標準化目的でない（つまり、Informatial/広報やexperimental/実験）RFCであるなら、RFCを出し変換IDが割り当てられる前に、IESGによって明確にレビューされ承認されなければならない。				
	IPSEC IPCOMP 変換IDは、ESPの前にIPレベルでの圧縮を提供するために使われる、ある一つのアルゴリズムを表わす8ビットの値である。新IPCOMP変換IDの割当の要求は、IPCOMPフレームワーク（[IPCOMP]）内でのアルゴリズムの使用方法を解説するRFCによらなければならない。付け加えて、要求されたアルゴリズムは公開され、かつパブリックドメイン(無償)でなければならない。				
	標準化目的でない（つまり、Informatial/広報やexperimental/実験）RFCであるなら、RFCを出し変換IDが割り当てられる前に、IESGによって明確にレビューされ承認されなければならない。				
	IPSEC SA 属性は、16ビットの種類とその値からなっている。IPSEC SA 属性は、様々な値をISAKMP 端間で受け渡すために使用される。新IPSEC SA 属性の割当の要求は、属性のエンコーディング（基本/可変長）とそのリーガル値を解説した、Internet Draft によらなければならない。				
	IPSEC IDは、可変長のIDペイロードの解釈を識別子として使用される8ビットの値である。新IPSEC IDの割当の要求は、IPSEC内でのIDの使用方法について解説するRFCによらなければならない。				
	標準化目的でない（つまり、Informatial/広報やexperimental/実験）RFCであるなら、RFCを出し変換IDが割り当てられる前に、IESGによって明確にレビューされ承認されなければならない。				
	IPSEC通知メッセージは、各DOIごとにISAKMPによって予約されている値の範囲から取られる16ビットの値である。エラーメッセージのために一 つの範囲(8192から16383)、状態メッセージのために別の範囲(24576032767)がある。新通知メッセージの割当の要求は、IPSEC内 でのそのIDの使用方法について解説する Internet Draft によらなければならない。				