IKEv1 のクイックモードによるフェーズ 2

●フェーズ 2 の通信は、セキュリティ処理された ISAKMP SA の使用（メインモードの**【③認証】**の時と同じ秘密対象鍵）により、ペイロード部分の暗号化が行われるため、安心して、IPsec SA に必要なパラメータの交換ができる。

●以下の①②の手順で IPsec SA を生成する。

【①】セキュリティプロトコル（ESP 又は AH）、暗号化アルゴリズム（AES 等）、認証アルゴリズム（HMAC-SHA1 等）、転送モード（トンネル又はトランスポートモード）等のネゴシエーションを行う。それと同時に互いの乱数を交換する。

【②】メインモード時に生成した 4 つの秘密対象鍵の内の 1 つ（メインモードの**【③認証】**の時とは違うもの）と互いに交換した乱数等から IPsec SA で使用する秘密対象鍵を生成。

IKEv2【IKEv1 からの変更点は以下のとおり】

●フェーズ 1 は IKE_SA_INIT、フェーズ 2 は IKE_AUTH

●エンティティ認証は、フェーズ 2 に相当する IKE_AUTH で行う。つまり、生成された IKE_SA で通信相手（端末機器等）を認証する。

●上記から IKE_SA_INIT でエンティティ認証を行わないので、フェーズ 1 の様に IP アドレスが固定とかの議論は不要になるので、結果的に IKE_SA_INIT ではメインやアグレッシブの区別はない。

●ISAKMP SA（上り下り兼用）は IKE SA（上り下り別々）、IPsec SA は Child SA

●IKE AUTH の転送モードにおいて、トンネルモードはデフォルトなので、トランスポートモード使用時のみ指定。

ESP と AH（トンネルモードの場合）

●IP ヘッダはプライベート IP アドレス、トンネル IP ヘッダはグローバル IP アドレス

●オリジナル IP パケット（OIPP）の並びは OIPP = IP ヘッダ + TCP ヘッダ + データ

●トンネルモードの先頭にはトンネル IP ヘッダ（TIPH）

●AH では、TIPH + AH ヘッダ（MAC 含む）+ OIPP となり、全てが認証範囲となる。

●ESP では、TIPH + ESP ヘッダ + OIPP + ESP トレーラ（暗号化の際のパディングに相当）+ MAC（ESP 認証データ）となり、黄色が暗号範囲、黄色に ESP ヘッダ を加えたものが認証範囲となる。

ESP と AH（トランスポートモードの場合）

●IP ヘッダは主にグローバル IP アドレス

●オリジナル IP パケット（OIPP）の並びは、トンネル IP ヘッダのように前に付くものはないが、

OIPP = IP ヘッダ + ブランク + TCP ヘッダ＋データ

●AH では、ブランクに AH ヘッダ（MAC 含む）を入れて完了となり、全てが認証範囲となる。

●ESP では、ブランクに ESP ヘッダ を入れて、

IP ヘッダ + ESP ヘッダ + TCP ヘッダ＋データ + ESP トレーラ（同上） + MAC（同上）となり、

トンネルモードと同様に黄色が暗号範囲、黄色に ESP ヘッダ を加えたものが認証範囲。

MAC（メッセージ認証コード）

●メッセージが長ければ暗号も長くなるが、MAC はメッセージの長さに関係なく固定長である。

●HMAC はざっくり言うと、［メッセージと MAC 鍵］のハッシュ値なので固定長になる。

●CMAC もざっくり言うと、ブロック暗号アルゴリズムに基づく MAC アルゴリズムを用いて、共通鍵（MAC 鍵）を使用してメッセージを固定長にする。

●CMAC は CBC-MAC 等のセキュリティ上の欠陥を修正したものである。CBC-MAC 等の CBC モードは、ひとつ前の暗号ブロックを次の段階でも使用するため、最後の段階で生成される暗号ブロックはメッセージ全体の要素が含まれることになる。そして、CBC モードの暗号ブロック長は固定長なので、それを CBC-MAC とすることで固定長になる。

●最近では、暗号化とメッセージ認証の同時処理を行う AEAD 暗号利用モード（AEAD）が普及しており、TLS1.3 では AEAD が必須で **AES-GCM** が多く使用される。GCM（Galois/Counter Mode）の Galois はガロア認証を指し、Counter Mode は暗号利用モードの CTR モード（**C**oun**T**e**R**）を指す。なお、CRYPTREC において、AES と GCM の組み合わせが推奨されている。

●WPA2 関連の推奨の認証及び暗号方式は、**AES-CCMP** である。CCMP（Counter-mode with CBC-MAC protocol）から、認証は CBC-MAC、暗号モードは CTR となる。

SSL/TLS

●SSL～TLS1.1 は使用すべきではない。TLS1.3 が現バージョンであるが、1.2 も現役。