IPsec-VPNの仕組み

メインモードのISAKMP SA

IKEフェーズ1

VPNクライアント

VPNゲートウェイ

暗号と認証方式の提案パラメタ		ISAKMPヘッダ	UDPヘッダ	IPヘッダ
IPヘッダ	UDPヘッダ	ISAKMPヘッダ	対応可能な暗号と認証方式	
クライアント側乱数	鍵交換パラメタ（DH公開値）	ISAKMPヘッダ	UDPヘッダ	IPヘッダ
IPヘッダ	UDPヘッダ	ISAKMPヘッダ	鍵交換パラメタ（DH公開値）	クライアント側乱数
クライアントハッシュ値	クライアントID	ISAKMPヘッダ	UDPヘッダ	IPヘッダ
IPヘッダ	UDPヘッダ	ISAKMPヘッダ	ゲートウェイヘッダ	ゲートウェイハッシュ値

暗号化

①ネゴシエーション

クライアントがISAKMPパラメタ（暗号化アルゴリズム、ハッシュアルゴリズム、認証方式など）を提案、ゲートウェイが対応可能なパラメタを選択。

②秘密対称鍵生成・交換

双方がDiffie-Hellman鍵交換アルゴリズムによって秘密鍵を共有し、それらをもとに4個の秘密対称鍵を生成。

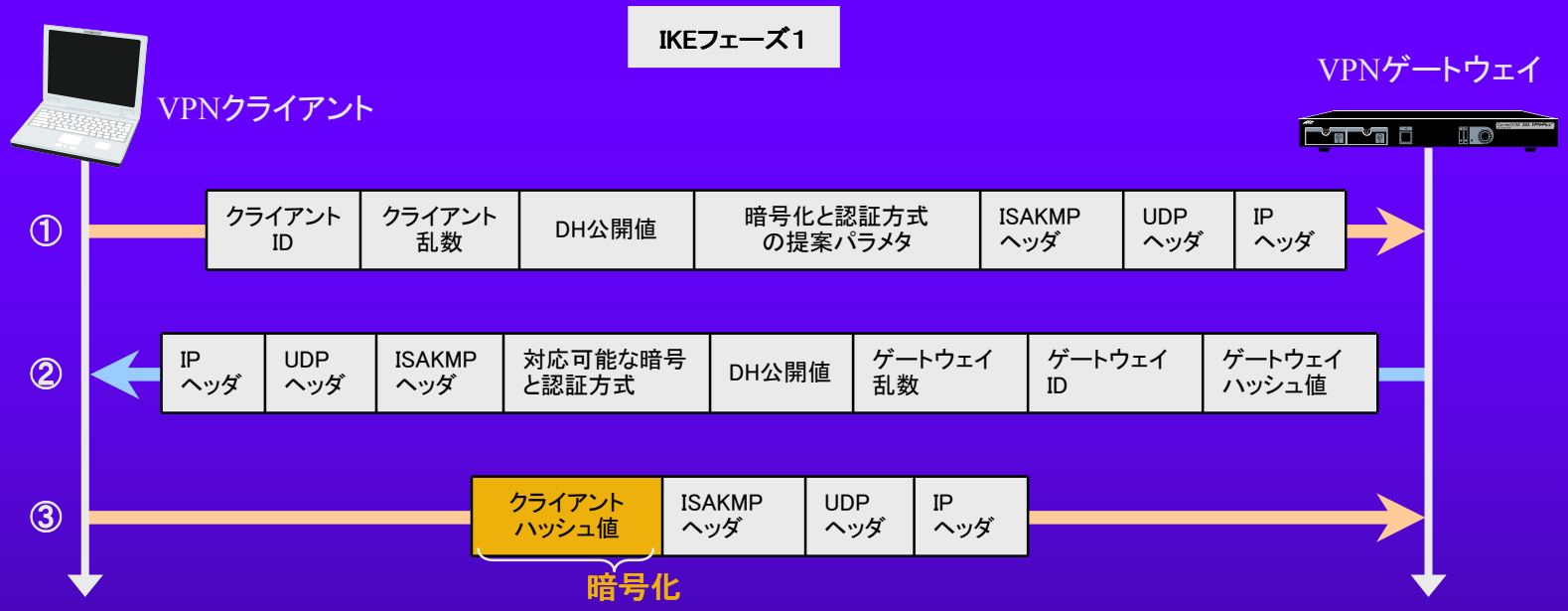
③相手の認証

IDと認証用のハッシュ値で相手を認証し、ISAKMP SAが確立。IDとハッシュ値は②で生成されたSKEYID_e鍵で暗号化される。

※IDにはIPアドレスしか使えない制約があり、動的にアドレスが変わる環境ではアグレッシブモードを用いる。

IPsec-VPNの仕組み

アグレッシブモードのISAKMP SA



①クライアントが、ISAKMPパラメタ、DH公開値、ID、認証用乱数を送信

秘密対称鍵を生成する前に最初のパケットでIDを送るため、暗号化はされない。

②ゲートウェイが、対応パラメタ、DH公開値、ID、認証用乱数、認証用ハッシュ値を送信

クライアントとゲートウェイがDH秘密鍵を共有し、メインモードと同様に4個の秘密対称鍵を生成。

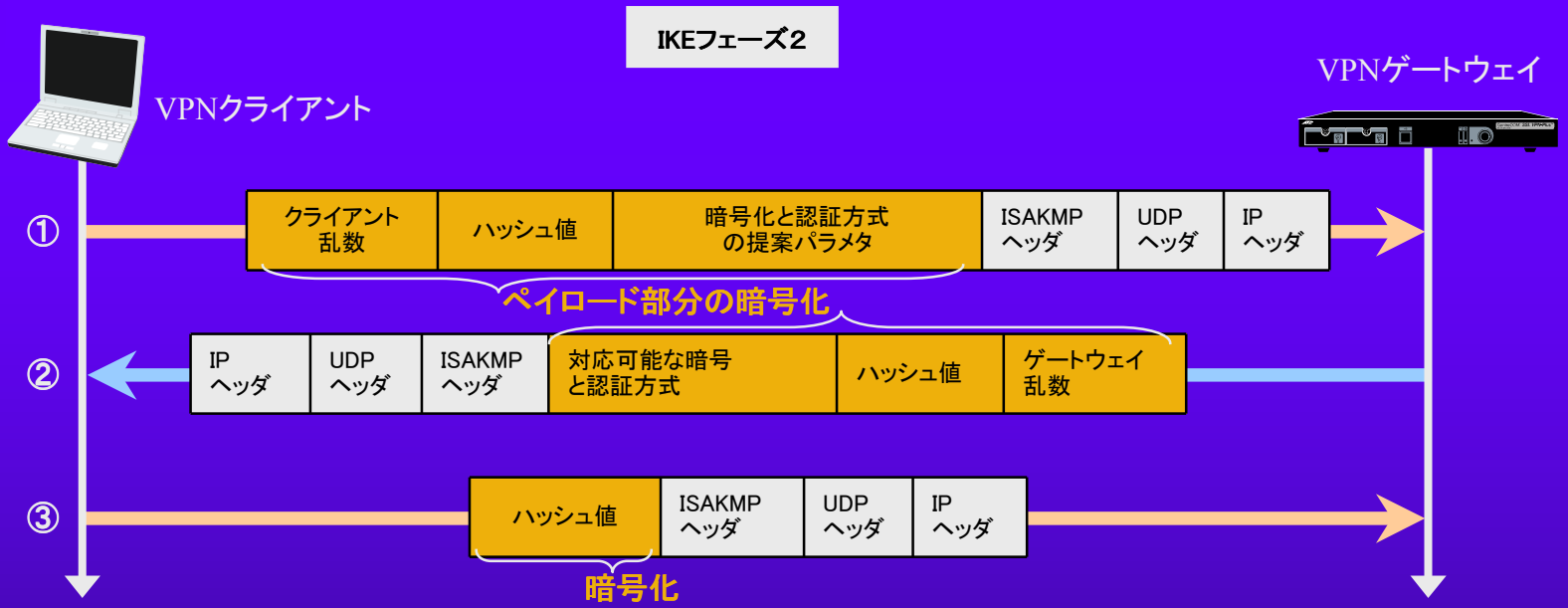
③クライアントが、認証用のハッシュ値をゲートウェイに送信

相手を認証し、ISAKMP SAが確立。ハッシュ値は②で生成されたSKEYID_e鍵で暗号化される。

※IDは暗号化されないが、FQDNなどを使用して事前共有鍵との対応付けを行う。それによりモバイルPC環境で利用可。

IPsec-VPNの仕組み

クイックモードによるIPsec SA



①クライアントが、IPsec SAパラメタ、認証用乱数、認証用ハッシュ値を送信

前フェーズで生成したSKEYID_eによって暗号化される。

②ゲートウェイが、対応パラメタ、認証用乱数、認証用ハッシュ値を送信

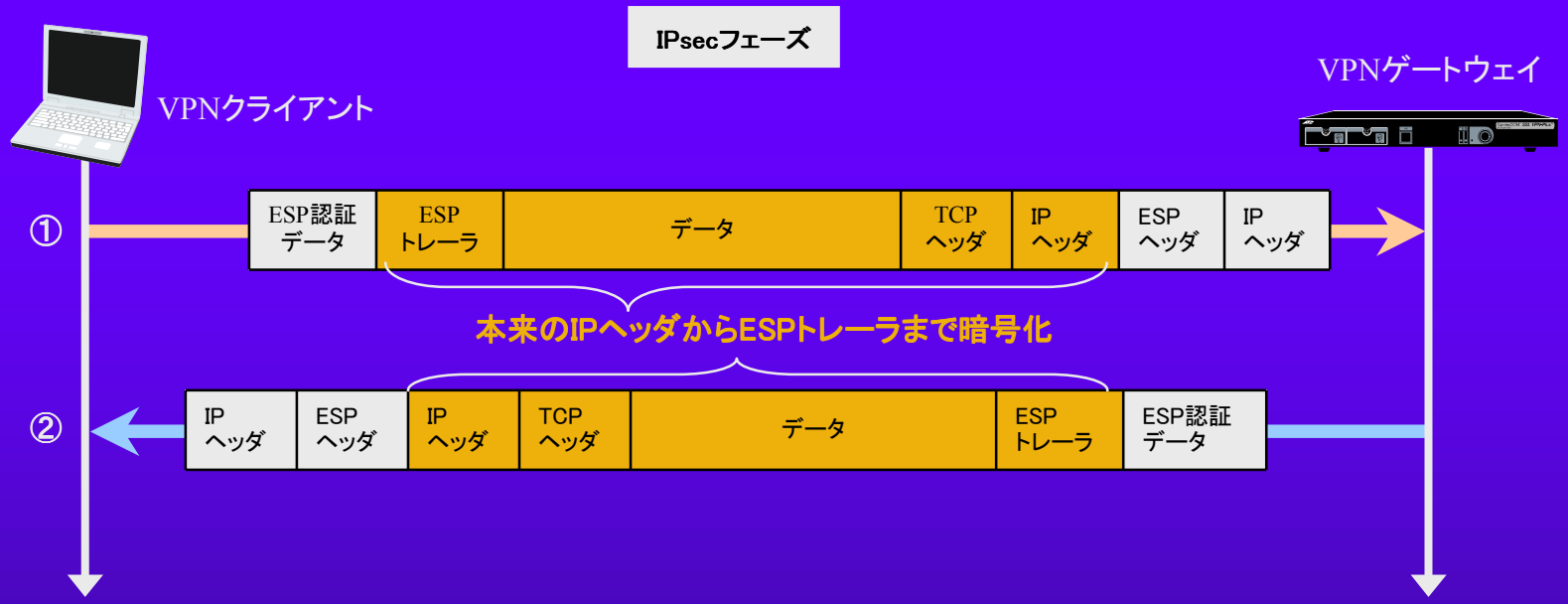
双方がSKEYID_d、SPI、クライアント認証用乱数、ゲートウェイ認証用乱数などからIPsec SAで使用する秘密対称鍵を生成。

③クライアントが、認証用のハッシュ値をゲートウェイに送信

相手を認証し、IPsec SAが確立。以降IPsec通信が可能となる。IPsec通信の開始後もSAが定期的に更新され、双方間で再認証と秘密対称鍵の更新が行われる。

IPsec-VPNの仕組み

SA確立後のIPsec通信（トンネルモード）



①クライアントからゲートウェイへの通信用トンネル（上り）

本来のIPヘッダからESPトレーラまで暗号化され、クイックモードによって築いたトンネル（IPsec SA）を通って通信する。先頭に付与されているのはトンネル通信用のIPヘッダである。通信前に暗号鍵で暗号化され、認証鍵で改ざんチェック用のハッシュ値（ESP認証データ）を付ける。ゲートウェイが受け取った暗号化部分は、共有している暗号鍵で復号し、認証鍵でハッシュ値を検証する。

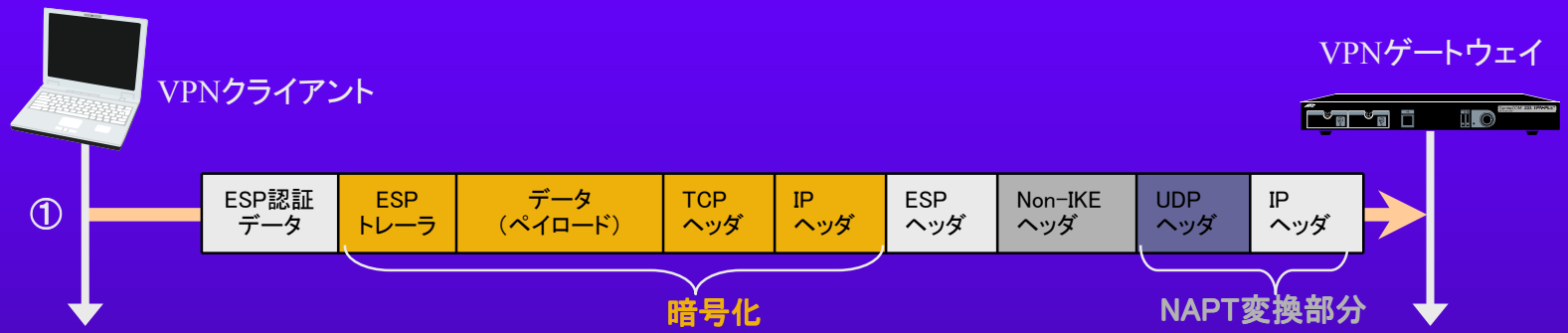
②ゲートウェイからクライアントへの通信用トンネル（下り）

ゲートウェイからも同様にクライアントへIPsecトンネル通信が行われるが、上りと下りのトンネルは異なる。トンネルごとに異なる暗号鍵・認証鍵がある。それらの鍵はIKEフェーズの2、IPsec SAで生成される。

IPsec-VPNの仕組み

IPsecのNAPT対応（NAT Traversal）

クライアントからゲートウェイ越しの社内LANへのアクセスは、NAPTを経由することが多い。通常、NAPTによってパケットのヘッダ情報が変更されるが、ポート番号はペイロードの一部として暗号化されており変換ができない。そのため、NAT Traversalなどの技術を用いてこの問題に対応する。



①クライアントからゲートウェイへの通信用トンネル（上り）

UDPヘッダを付与することでカプセル化し、IKEと同じポートを使用することでファイアウォールの修正なしで通信を行う。本来のIKEパケットと区別するため、「Non-IKE」フラグをセットする。