# 5. 相互接続特性の分析

製品個々の設定に「ノウハウ」と呼べるようなパラメータ設定の「癖」が存在する。今回の実証実験ではこれらを大きくまとめようと試みたが、現状の製品群では結局個々の製品設定の特性として意識せざるを得ない結果となった。

詳細は付録 C「製品ごとの相互接続特性」に各製品ごとに特性事項として収録したのでそちらを参照されたい。

# 6. まとめ

## 6.1.　はじめに

今回の相互接続試験は、これまでに実施されてきた相互接続試験と比較し参加機器数が非常に多いため、実施した全ての試験において全ての組合せの試験をくまなく実施する事が出来なかった。これは、参加ベンダーの技術者の時間的制約も原因の一つではあったが、試験の運営を行なった JNSA 相互接続ワーキンググループの試験運営方法にも課題があり、今後の試験を継続実施する上で解決してゆかなければならない。

## 6.2.　試験考察

① 基本接続性

基本接続性試験では標準で実装必須となっている Pre-Shard 相互認証方式を使用した異機種間の相互接続性の確認を行った。結果は試験を実施したすべての組合せで接続を確認することができた。しかし、機器間ごとにネゴシエーションから IPSec 通信が開始されるまでの所要時間に大差があることがこの試験を通して判明した。今後の試験ではこれについても確認が必要である。

② フェーズ 2 における ID ペイロードタイプ

フェーズ 2 の ID ペイロードタイプは、IPSec 通信に先立って構築される SA を「Host」単位で構築するか、「Subnet」単位で構築するかを決定する項目である。通常の機器では構築可能な SA の数に制限があるため、「Subnet」単位で SA を構築することが多い。

今回の試験結果では、この ID ペイロードタイプが異なっていても通信できる組合せ多かったが、本来の目的から考えると「Host」と設定されている機器が Responder となった際に、「Subnet」と設定されている機器から通信要求があった際には通信を拒否する必要があると考える。「Host」と設定されている機器は SA を「Host」単位で構築するため、Peer のサブネット上の端末ごとに SA を構築することとなり、必要以上に SA が構築され最悪の場合、機器がダウンする事態を招くことが考えられるからである。今回の試験ですべての組合せで接続可能であった製品が実際にどのような SA を構築していたかどうかを確認していなかったため、前述の問題が実際に発生するかどうかはわからないが、今後の試験では異なるペイロードタイプを使用したときに、実際にどのような SA が構築されているか確認が必要である。

③ Re-key 動作

通信中に Re-key が発生した際に IPSec 通信が維持されるかどうかを確認した。IPSec 通信に必要な SA はセキュリティレベルを保つために、有効期限(Life Time)が設定されている。通信中にこの Life Time を迎えた際に SA を更新する動作を Re-key と呼ぶ。

今回の試験で「×」がついている組合せについては、Re-key 動作失敗しそれ以降 IPSec 通信が実施できないことを意味するため、運用時には大きな問題が発生することが考えられる。一方「◎」と「○」は Re-key 動作には問題ないことを表しているが、Initiator と Responder で異なる Life Time を使用した際に、採用される Life Time が組合せによってさまざまである事と、構築された SA の残有効期限がどれくらいの値になったら Re-key を実施するかが製品によって異なるため、双方向で Re-key が確認できた組合せと、一方向のみで Re-key が確認できた組合せに分かれる結果が得られた。これらの採用される Life Time と Re-key 動作のタイミングについては、各機器の「動作仕様」を参照されたい。

④ IP フラグメント処理

IPSec 機器が ESP 処理を実施した際に IP フラグメンテーションが発生する条件でどのような動作を行うかを確認した。一つ目の確認として、元のパケットを ESP にカプセリングした際にフラグメントが発生するパケットを各 IPSec 機器がどのように処理するかを確認した結果、Don't Fragment がセットされていない場合は、各 IPSec 機器はパケットをフラグメントして通信しているが、Don't Fragment がセットされた場合、ハードウェア製品はそのパケットをフラグメントして通信し、ソフトウェア製品はフラグメント処理せず送信元に ICMP メッセージを返している傾向が確認できた。どちらの動作が正しいかの判断は IPSec 標準に明確な記述がないため判断できないが、使用用途によっては Don't Fragment ビットがセットされている場合に IPSec 機器がパケットをフラグメントして通信すると問題が発生する可能性があることは付け加えておく。
また、もう一つの確認項目として PMTU があるが、今回の試験環境では PMTU のサポート状況を正確に確認することができない環境であったため、今後の試験の課題とする。

⑤ SA 消失時の回復手順問題

IPSec 機器を運用する際に一番大きな問題となるのが、構築された SA が一方の機器で消失しその結果 IPSec 通信が不能となる場合である。このような事態が発生した際に、どのような手順を踏んで作業を実施すれば SA を回復することが可能かどうかを確認するためにこの試験を実施した。
管理者の理想ではそのような事態が発生した際にも、意識することなく自動的に SA が回復されることが望ましいが、先にも述べたように IPSec 標準ではエラー発生処理が明確に規定されていないため、自動的に SA が回復したことを表す「◎」がほとんど無いのが現状である。「◎」の結果を多く収めている製品は Peer から Information を受信した際に、それに伴う動作をおこなっていた事がわかっている。一方「○」の結果が得られた製品では、SA が削除されたほうから通信を開始することで SA が回復できることが確認できた。現状では最低限「○」の結果が得られない組合せでは運用時に問題が発生する可能性が高いと考える。

⑥ END to END の通信確認

FTP と TFTP を使用して、TCP と UDP の End to End の通信確認試験を実施し、FTP については実際の運用を考慮しファイル転送中に Re-key 動作を行わせた。ほとんどの製品で「○」の結果が得られたが、「×」の結果が得られた組合せについては Re-key 動作後に通信不能となっていることが確認できた。この原因の一つとして、Re-key 動作に時間がかかりその結果 FTP がタイムアウトしていた事が考えられる。今後の試験ではよりタイムアウトに厳しいアプリケーションで試験を実施する必要がある。また、今回は実施できなかったが今後益々使用されるマルチメディア系のアプリケーションを使用した試験も実施する必要があると考える。

## 6.3. 総評

基本試験/相互接続性確認試験は、国内市場で購入可能な製品の相互接続性の確認を目的として行った。異機種間の接続性は試験結果が表すように、IPSec 製品が市場に出回り始めた 2 年ほど前と比較し大幅に向上している事がわかり、一定の成果を挙げることができたと考える。

基本試験/運用性確認試験は、IPSec 機器の機種や機能に関わらず IPSec 機器を運用する際に必要な情報を収集する事を目的として行った。各試験の結果では機器による大差はなく概ね良好な結果が得られているように見える。しかし実際にはマニュアル等では確認できない各機器の動作の差異があり、これが相互接続を困難にさせている。今回の試験では各機器の動作差異を「動作仕様」にまとめることができた。この点は、今回の試験の大きな成果であると考える。

試験を通して再認識させられる結果となったが、異機種間の相互接続はまだまだ問題が多く残されており、運用には相応の知識と労力が必要となる。このような現状を招いている大きな要因として IPSec 標準に「あいまい」な記述が多いことが挙げられるが、これらが修正され各機器がそれを実装するまで待つことはできないため、JNSA としては異機種間の相互接続環境を運用する際に実施すべき「検証項目」と「判断基準」を明確にすることが今後の最重要課題であると考える。

## 6.4. 補足（機器選定の目安）

市場に出回っている多くの IPSec 機器から使用用途に応じた機器を選定するのは、IPSec を使用した経験がないと非常に困難である。この報告書のまとめとして今後 IPSec を使用した VPN を構築する際の機器選定のポイントを解説する。

機器を選定する際の最初のステップとして、「どのような場所」で「どのように使用」するのかを明確にする必要がある。どのような場所でというのは、トラフィックが集中するセンター側で使用するのか、SOHO サイトで使用するかを明確にする事である。どのように使用するのかというのは、IPSec 専用機器を使用するのか、ファイヤーウォール兼用機として使用するのか、それともルータ兼用として使用するのかを明確にすることである。この 2 つを明確にすることによって使用可能な機器がある程度が絞られてくる。次に確認すべき項目は通信相手数である。IPSec 専用機の多くは構築可能な SA の数に制限があり、これによって同時接続可能なサイト数が制限される。また機器によって 10/100Mbps のインターフェースを実装していても、実際の IPSec 通信時のスループットが数 Mbps となっている製品が多いのでこれについても確認が必要である。ここまでは IPSec 機器を運用した経験や、機器のカタログ等を確認することで比較簡単に行える作業である。

次に運用の視点から製品選定の目安を考えると、以下の項目の確認が必要である。

- 設定変更時の SA 状況
- SA 削除機能のサポート
- Life Time の設定方法
- SA 回復手順

各項目について順に解説する。

◆設定変更時の SA 状況について

機器によっては設定変更を行うとそれまでに構築した SA をすべて削除してしまう製品がある。このような機器は設定変更がほとんど無いサイトや、SOHO サイトで使用することが望ましい。数多くのサイトと SA を構築するセンターサイトや、設定変更が頻繁に発生するサイトで使用すると、設定変更の度に SA が消失してしまうため SA 回復の作業が必要となるためである。

◆ SA 削除機能のサポート

一方の SA が消失したために IPSec 通信が不能となった場合など、SA を削除しなければならない状況が発生する。このような場合、コマンドや GUI ツールなどから SA が削除可能な機器であれば簡単に対応することができる。またこのような機能を持っていなくとも、機器を再起動することで SA を削除することは可能である。しかし、トラフィックが集中するサイトで再起動に

よる SA 削除を実施すると、正常な SA まで削除することになってしまい一層問題を大きくする可能性があるため、センター側などのトラフィックの集中するサイトで使用する機器は Peer 毎に SA を削除する機能を有する製品を選定すべきである。

◆Life Time の設定方法

通常 IPSec 機器を運用する場合、通信相手との Life Time は同じ値に設定する。しかし機器によっては Phase1 SA が固定値になっているものもあるので、通信を行う相互の機器で IKE SA と IPSec SA の設定可能な Life Time 値を確認し同一の値を設定可能であることを確認する必要がある。もしも、通信を行う相互の機器で同じ値を使用することができないと、SA 有効期限切れが原因で一方の SA が早く消失してしまい、SA 回復作業を実施する必要がある。

また、複数の大規模な VPN 網で使用を検討する場合は、VPN 網事に使用している Life Time 値が異なることが考えれらるため、Peer 毎に Life Time が設定可能かどうかを確認する必要がある。

◆SA 回復手順

一方の SA が消失し IPSec 通信に障害が発生した場合、どのような手順を行えば SA を回復できるかを確認する必要がる。IPSec 機器を運用中に発生する障害のほとんどは、一方の SA が消失したことに起因する障害であるため、この回復手順は事前確認必須の項目であると考える。

これら以外にもリモート管理機能サポートなど多くの項目があるが、上記の項目を確認することにより運用中に発生する問題の多くを未然に防ぐことが可能であると考える。しかしこれらの情報はカタログ等には記載されていない項目ばかりであるため、ベンダーからの情報提供が必要になるため、異なるメーカの機器を使用した VPN 構築を成功させるには、豊富な知識と経験をもつベンダーの協力が必須であるのが現状である。