ネットワークにつながらない理由

ネットワーク機器編

第2回

インターネットVPNで使うルーターのトラブル解決

WAN越しのVPN接続を確認 IPsecの動作状況と設定を見直す

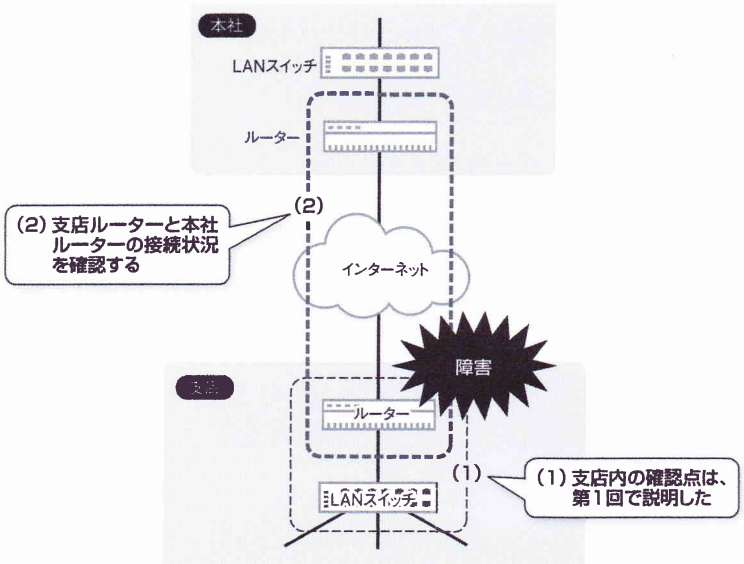
NECフィールディング
サービス技術本部
マルチソリューション技術部
主任
小沢 広人（おざわ ひろと）

前回は、「拠点内にあるパソコンから本社サーバーにアクセスできない」という現象から、障害の被疑箇所を支店内に設置した拠点ルーターの周辺に絞り込んだ。そのうえで、拠点ルーター自身の基本動作とその両隣に設置されている機器との接続状態を確認した。今回はインターネットVPNを介した本社ルーターとの接続状態を、拠点ルーター側から確認する方法を説明する（図1）。

拠点ルーターと本社ルーターの接続を確認する方法を説明する前に、インターネットVPNで使うIPsecトンネルの動作を理解しておきたい。基本動作を理解しておくと、原因の切り分け作業を的確かつ効率的に実施できる。

図1 ルーターで発生したトラブルの切り分け方

LAN側に異常がない場合は、本社ルーターとの接続状況を確認する。



IPsecの基本動作を理解しておく

IPsecは、IPパケットに対しデータの暗号化とメッセージ認証を実施して、インターネット上でもセキュリティを確保した通信を行うためのプロトコルである。データの暗号化とは、ネットワークを通じてデータをやり取りする際に、途中で第三者に盗聴されてもパケットの内容がわからないようにデータを加工する処理だ。メッセージ認証とは、悪意ある第三者がパケットの中身を改ざんした際に、それを検知する仕組みである。

パケットで暗号化を施す箇所は、使用するモードによって異なる。IPsecには「トンネルモード」と「トランスポートモード」の二つのモードがある。トンネルモードは、IPヘッダーを含むIPパケット全体を暗号化するモードで、データ部だけではなくIPパケット送受信者のアドレスも外部から隠すことができる。トランスポートモードは、IPパケットのデータ部のみを暗号化するモードである。拠点間のインターネットVPNでは、前者のトンネルモードがよく使用される。

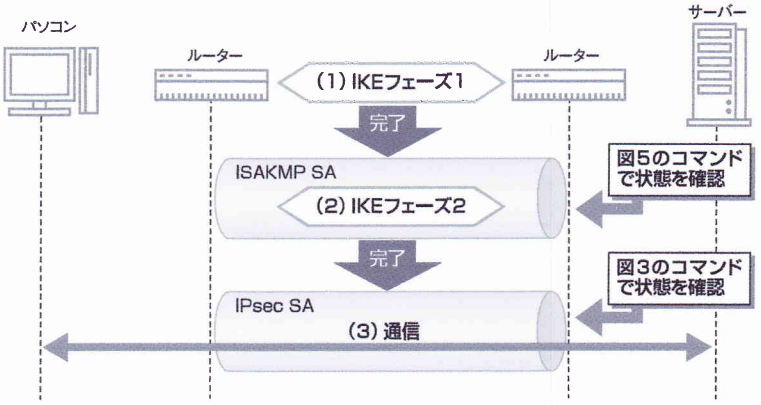
IPsecを使って暗号化データ通信をするためには、IPsec通信をする機器同士がSAと呼ばれるコネクションを確立し、通信で使用する暗

号/認証方式や、暗号/認証処理に使う秘密鍵の整合性を取る必要がある。SAはあらかじめ手動で設定しておくことも可能だが、セキュリティを高めるためと定期的な設定変更の手間を省くために自動生成するほうがよい。そこでIPsecでは、SAを自動生成できる自動鍵管理プロトコル「IKE」(Internet Key Exchange)を定めている。今回は、現在一般的に使用されているIKEv1を前提に説明を進める。

まずはIKEv1の動作について少し触れておく。IKEv1によってSAが生成されるまでには、二つの段階(フェーズ)を経る。フェーズ1は、ISAKMP SAを構築する「ISAKMP SAの折衝」である。ISAKMP SAは、IPsec SAを確立する前段階として、IPsec SAで使用するパラメーターを保護する目的で使われる。フェーズ2は、IPsec SAを構築する「IPsec SAの折衝」である(**図2**)。IPsecトンネルを使用して拠点間通信を行うまでの基本動作をまとめると、次のような流れになる。

(1) ルーター同士でIKEv1のフェーズ1によるISAKMP SAの折衝を実施する
(2) ISAKMP SAを使用して、ルーター同士でIKEv1のフェーズ2によるIPsec SAの折衝を実施する
(3) IPsec SAを使用して、ルーター間で暗号化データ通信を実行する

図2 IKEv1の動作概要
二つのフェーズを経て、セキュリティを確保するコネクションであるIPsec SAを生成する。



(1) IKEフェーズ1:ISAKMP SAの折衝を行う
(2) IKEフェーズ2:ISAKMP SAの保護の下、IPsec SAの折衝を行う

IKE:Internet Key Exchange
ISAKMP:Internet Security Association and Key Management Protocol
SA:Security Association

図3 IPsec SAの生成状態を確認する
「show ipsec sa」コマンドを使う。

■IPsec SAが生成されている場合

```
Router(config)# show ipsec sa ------IPsec SAの状態を表示させるコマンド
IPsec SA - 1 configured, 2 created ------IPsec SAが生成されていることを示す
(以下省略)
```

■IPsec SAが生成されていない場合

```
Router (config)# show ipsec sa
IPsec SA - 1 configured, 0 created ------IPsec SAが生成されていないことを示す
(以下省略)
```

これを踏まえて、IPsecによるインターネットVPNで発生したトラブルを切り分ける方法を見ていく。

IPsec SAの生成状態を確認する

まずは、本社ルーターにアクセスできない原因がIPsec通信にあるかどうかを切り分けるため、IPsec SAの生成状態を確認する。IPsec SAが生成されていない場合は、IKEの動作に異常があることが考えられる。IPsec SAが生成されていれば、その生成に必要な通信が拠点ルーターと本社ルーターとの間でできていることになるため、インターネット回線に問題が発生している可能性を除外できる。つまり問題はIPsecやIKE以外にある可能性が高い。

このケースでは、拠点ルーターのルーティング設定に問題がある可能性を疑う。例えばNECのUNIVERGE IX2105では、IPsecをトンネルモードで利用する際には、IPsec通信用の論理的なインタフェース(トンネルインタフェース)を使用する。IPsecの暗号化対象となるパケットはこのトンネルインタフェースから出力するので、ルーターにそのためのルーティング設定を投入しなければならない。このルーティング設定がされているかどうかを確認する。

IPsec SAの生成状態を確認する方法はルーターのベンダーや機種によって異なる。UNIVERGE IX2105では、「show ipsec sa」コマンドを使ってIPsec SAの生成状態を確認できる。**図3**はその実行結果である。「IPsec SA

▼IPsec
security architecture for IPの略。
▼SA
Security Associationの略。あるトラフィックのセキュリティを確保するコネクションのこと。
▼IKEv1
IKE version 1の略。

▼pingコマンド
IPレベルでの通信状況（疎通）を確認するためのネットワークコマンド。

が生成されていない場合」の項目にある2行目を見てほしい。ここに「0 created」という表示があれば、IPsec SAは生成されていないことがわかる。

またUNIVERGE IX2105では、IPsec SAが一つ以上確立していれば装置前面の「VPN」ランプが緑点灯する。そのためコマンドを使わなくても、このランプの状態が消灯している場合は、IPsec SAが全く生成されていないと判断できる（図4）。

IPsec SAが生成されなければIKEを確認

IPsec SAが生成されていないことが判明したときは、IKEv1のどのフェーズに問題があるのかを確認する。まず、IKEフェーズ1が正常に完了していないなら、拠点ルーターと本社ルーターの間でISAKMP SAが生成できていないことになる。IKEフェーズ1は成功しているもののIKEフェーズ2が正常に完了していないときは、拠点ルーターと本社ルーターの間でIPsec SAを確立するのに必要な暗号/認証方式などのパラメーター設定に誤りが含まれている可能性がある。

UNIVERGE IX2105では、「show ike sa」コマンドでISAKMP SAの生成状態を確認できる（図5）。show ipsec saコマンドの実行時と同様に、「0 created」と表示されている場合、ISAKMP SAは生成されていない。つまりフェーズ1は完了していない。

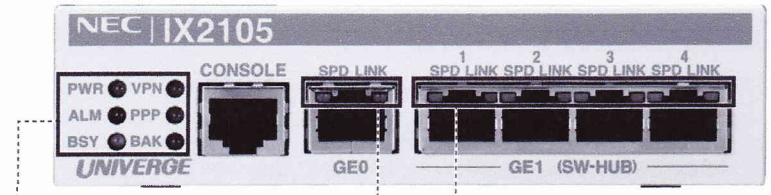
IKEフェーズ1が完了しない原因の一つとして、拠点ルーターと本社ルーターがそもそも通信できない状態にあることが考えらえる。これを切り分ける方法として、まず拠点ルーターから本社ルーターに対してpingコマンドを実行して、きちんと応答があることを確認する。応答がなければトラブルの原因はIPsec/IKE以外であり、さらにインターネット回線も含めた切り分け作業が必要になる。拠点ルーターと本社ルーターのIPアドレスやルーティングの設定に誤りがないことを確認し、次にルーターを設置した両拠点で、インターネット回線に接続できることを確認する。インターネット回線へ接続できない原因は、回線事業者側にあることも考えられる。そのため回線事業者に、トラブルが発生していた日時に回線工事をしていなかったか、また回線故障が発生していなかったのかを問い合わせる。

UNIVERGE IX2105では、PPP（Point-to-Point Protocol）のセッション確立時に装置前面にある「PPP」ランプが緑点灯する。回線がPPPoE（PPP over Ethernet）接続を使用しているケースでは、このランプで回線の接続状態を確認できる。PPPランプが消灯している場合は、PPPoEの接続設定が正しいかどうかを確認する。

フェーズ1が完了しないもう一つの原因として、拠点ルーターと本社ルーターでISAKMP SAを確立するために必要な暗号/認証方式などのパラメーター設定に誤りが含まれている可能

図4 ルーターが搭載している状態表示ランプの例

写真はNECの「UNIVERGE IX2105」の前面である。本社ルーターとの接続状態は、「VPNランプ」「PPPランプ」を注意してみるとよい。



PWR：電源投入時に緑点灯
ALM：異常検出時に赤点灯
BSY：FLASHメモリー書き込み中に橙点滅
VPN：IPsec SA（コネクションのこと）確立時に緑点灯
PPP：PPPセッション確立時に緑点灯、接続中に緑点滅
BAK：ネットワークモニター機能で障害検出時に緑点灯（設定が必要）

SPD：100M動作時に緑点灯、1G動作時に橙点灯
LINK：リンク確立時に緑点灯、送受信中に橙点滅

図5 ISAKMP SAの生成状態を確認する

「show ike sa」コマンドを使う。

■ISAKMP SAが生成されている場合

```
Router(config)# show ike sa
ISAKMP SA - 1 configured, 1 created
（中略）
  #ph1 success: 1, #ph1 failure: 0
  #ph1 hash err: 0, #ph1 timeout: 0, #ph1 resend: 0
  #ph2 success: 1, #ph2 failure: 0
  #ph2 hash err: 0, #ph2 timeout: 0, #ph2 resend: 0
```

show ike sa：ISAKMP SAの状態を表示させるコマンド
1 created：ISAKMP SAが生成されていることを示す
フェーズ1の統計情報
フェーズ2の統計情報
success：成功数　failure：失敗数
hash err：ハッシュエラー数
timeout：タイムアウト回数
resend：再送パケット数

■ISAKMP SAが生成されていない場合

```
Router(config)# show ike sa
ISAKMP SA - 1 configured, 0 created
（以下省略）
```

0 created：ISAKMP SAが生成されていないことを示す

図6 IKE関連のイベントログを確認する イベントログはあらかじめ設定しておく必要がある。またinfo/debugレベルのイベントログは装置の負荷が大きいため、障害切り分け時のみ設定する。

■イベントログを記録する設定

```
Router(config)# logging buffered ---------- ログを不揮発性メモリーに保存する設定
Router(config)# logging timestamp datetime ---------- ログに日付を付加する設定
Router(config)# logging subsystem ike info ---------- IKE関連ログを「info」レベルで出力する設定
```

pingコマンドなどで通信を発生させたあと、show loggingコマンドでイベントログを確認する

■イベントログを確認するコマンドと実行結果

```
Router(config)# show logging ---------- イベントログを確認するコマンド
```

●正常にフェーズ1、フェーズ2ともに完了した場合

```
2012/xx/xx 13:35:30  IKE.001: Begin IKE phase 1 negotiation, destination xx.xx.x.x ------- フェーズ1開始
2012/xx/xx 13:35:30  IKE.002: Finish IKE phase 1 negotiation, destination xx.xx.x.x ------ フェーズ1完了
2012/xx/xx 13:35:30  IKE.001: Begin IKE phase 2 negotiation, destination xx.xx.x.x ------- フェーズ2開始
2012/xx/xx 13:35:30  IKE.002: Finish IKE phase 2 negotiation, destination xx.xx.x.x ------ フェーズ2完了
```

(a)フェーズ1を開始したが、相手から応答がなく完了していない場合(「Receive」や「Finish」が表示されない)

```
2012/xx/xx 13:44:57  IKE.001: Begin IKE phase 1 negotiation, destination xx.xx.x.x --- 本社ルーターに情報が届いていない可能性があるため、「destination」に続くIPアドレスにpingが通ることを確認する
```

(b)フェーズ1を開始しているが相手からのエラー通知を受信し、フェーズ1の折衝がうまくいかない場合

```
2012/xx/xx 13:50:59  IKE.001: Begin IKE phase 1 negotiation, destination xx.xx.x.x
2012/xx/xx 13:50:59  IKE.009: Receive notification data from xx.xx.x.x
type 14:NO-PROPOSAL-CHOSEN, protocol ISAKMP ---------- 「選択できる提案がない」ことを通知された。これはISAKMP SAに関するパラメーターが誤っている可能性がある
```

(c)フェーズ1は完了しフェーズ2を開始しているが相手からのエラー通知を受信し、フェーズ2の折衝がうまくいかない場合

```
2012/xx/xx 14:01:56  IKE.001: Begin IKE phase 1 negotiation, destination xx.xx.x.x
2012/xx/xx 14:01:56  IKE.002: Finish IKE phase 1 negotiation, destination xx.xx.x.x
2012/xx/xx 14:01:56  IKE.001: Begin IKE phase 2 negotiation, destination xx.xx.x.x
2012/xx/xx 14:01:56  IKE.009: Receive notification data from xx.xx.x.x,
type 14:NO-PROPOSAL-CHOSEN, protocol ISAKMP ---------- 「選択できる提案がない」ことを通知された。これはIPsec SAに関するパラメーターが誤っている可能性がある
```

■イベントログの設定を削除するコマンド

```
Router(config)# no logging buffered
Router(config)# no logging timestamp datetime ---------- 設定を削除する場合は、最初に「no」を付けてコマンドを実行
Router(config)# no logging subsystem ike info
```

性がある。また、IKEv1はUDPの500番ポートで通信をするため、ルーターにUDP500番ポートの通信を許す設定がされている必要がある。このことを含めて、設定を再確認することが必要だ。

なおルーターによっては、IKEのどの処理が失敗しているのかを、ログで確認できる。UNIVERGE IX2105では、IKEの処理状況を「イベントログ」に残すことができる。初期設定ではイベントログを記録しない設定になっているため、前もってイベントログを取得する設定に変更しておかなくてはならない。この場合は**図6**の「イベントログを記録する設定」の部分に示したコマンドを入力すればよい。ここでは、IKEに関連するログを「info」という詳細なレベルで出力するよう設定している。この設定を行ったうえで「show logging」コマンドを実行すると、IKEv1のフェーズ1/フェーズ2の実施状況が表示される。以下にいくつかの例を挙げる。

(a) フェーズ1を開始したが、相手から応答がなく完了していない

▼UDP
User Datagram Protocolの略。IP上で動作するプロトコルで、低遅延を実現できる。

▼レベル
レベルが高いほうから、error、warn、notice、info、debugの5段階がある。IX2105ではこれを「メッセージレベル」という。

▼MTU
Maximum Transmission Unitの略。

▼MSS
Maximum Segment Sizeの略。

▼TCP
Transmission Control Protocolの略。IP上で動作するプロトコルの一つで、信頼性を確保する仕組みを備える。

(b) フェーズ1を開始しているが相手からのエラー通知を受信し、フェーズ1の折衝がうまくいかない
(c) フェーズ1は完了しフェーズ2を開始しているが相手からのエラー通知を受信し、フェーズ2の折衝がうまくいかない

(a) のメッセージからは、本社ルーターに情報が届いていない可能性が考えられる。そこでSAの折衝相手、つまり図6に示すイベントログの「destination」のあとに表示されるIPアドレスに対してpingコマンドが通るかどうかを実行し、応答があることを確認する。(b) の場合は、IKEフェーズ1のやり取りの最中に本社ルーターから「選択できる提案がない」というエラー通知が送られてきている。ここからISAKMP SAに関するパラメーターが誤っている可能性が読み取れるため、これを見直す。(c) のエラー通知は(b) と同じ内容だが、IKEフェーズ2に関するやり取りの最中に送られてきていることから、IPsec SAに関する暗号/認証方式などのパラメーターを確認する。

ここで使用するinfoレベルのイベントログは、設定できる5段階のレベルのうち、2番目に低いレベルである。レベルを低く設定するにしたがって、詳細なイベントログを確認できる一方で、取得するイベントの量が増加する。infoレベルのイベントログを取得する際にUNIVERGE IX2105に大きな負荷がかかるため、レベルの低いイベントログは障害切り分け時のみ取得するように設定したい。切り分け作業が済んだら、図6の下のほうに示すように「no」を付けてコマンドを実行して、イベントログを記録する設定を削除する。イベントログを常時取得するときは、レベルの高い「error」または「warn」レベルに設定することをお勧めする。warn以上のレベルであれば、取得するイベントが限定されるので、ルーターにかかる負荷も少ない。

図7 コンフィグ情報など、基本的な情報を一括で収集する
「show tech-support」コマンドを使用する。

```
Router(config)# show tech-support ---------- 基本情報を一括表示するコマンド
Calculating configuration memory size...
-------------------- show clock --------------------
Monday, xx March 20xx xx:xx:xx +09 00
  :
(以下省略)
```

イベントログを表示させるshow loggingコマンドを除き、連載で紹介した状態表示コマンドはすべてshow tech-supportに含まれる。
- show error-log (show crashinfoとして表示)
- show startup-config
- show interfaces detail
- show utilization
- show utilization history
- show ipsec sa
- show ike sa

設定は正しいが通信が不安定なときは

IKEの設定は正常に完了したものの、いざIPsec通信を開始すると通信が不安定になってしまうことがある。その原因として考えられるのは、パケットの分割(フラグメント化)処理である。

通信ネットワークでは、1回で送信できるフレームの最大値が決められており、この値をMTUと呼ぶ。フレームのサイズがMTU値を超過すると、自動的に分割して送られる。これはIPのパケット長にも影響する。IPsecの暗号化処理を行ったIPパケットは、暗号通信用のヘッダーをIPパケットに付け足すため、元のIPパケットと比較してサイズが大きくなる。これがロングパケット(またはラージパケット)と呼ばれる規定サイズぎりぎりの大きなパケットだと、暗号化処理によりMTU値を超えることがある。この場合、パケットはルーターでフラグメント化される。

ところがIPパケットのヘッダーに「フラグメント禁止」の設定がされていると、ルーターはパケットのフラグメント化を実行できない。かつMTU値を超えているため転送することもできず、ルーターはIPパケットを破棄してしまう。その結果、一部のパケットが欠落して通信が不安定になる。

このような現象を確認したら、次の二つの回避策を実行する。

・ルーターでMSS値を書き換える

MSSは、IPの上位層に当たるTCPで受信可能な最大のセグメントサイズを示す値である。IPsecで処理された後のサイズを考慮してMSSをルーターで書き換える設定に

しておくことで、TCPコネクション確立時に通常より小さなMSS値をパソコンやサーバーといったホストに通知することができる。その結果、クライアントはこれに沿ったサイズのTCPデータを送り出すため、IPパケットのサイズがMTU値より大きくなることはない。ただしMSS値はTCPだけに有効であり、UDPなどその他のプロトコルには効果がない点に注意が必要だ。

・ルーターで強制的にフラグメントする

IPsecの処理後に強制的にフラグメントするようにルーターを設定する。この設定により、IPパケットのヘッダーでフラグメントを禁止する設定になっていても、ルーターはIPsecの処理後にパケットをフラグメントして送信する。

普段からの準備と予防も大事

本連載ではここまで2回にわたって、インターネットVPNで使うルーターのトラブルシューティングを紹介してきた。トラブルの解決方法は様々で、ケースに応じて変わる場合もあるが、ここで紹介したトラブル解決方法が一つの参考になれば幸いである。どのような手段を用いてもトラブルをゼロにすることはできないので、トラブルが発生したら迅速に復旧作業を始められるように準備とトラブル予防を行うことが大切である。

最後にUNIVERGE IX2105を例に、日頃から実践しておくとよい準備と、故障を予防する方法を紹介しておく。まずトラブル対応のための準備としては、以下の3点を挙げておきたい。

(イ)コンフィグのバックアップ
(ロ)正常時のインタフェース状態の把握
(ハ)正常時のシステムロードアベレージの把握

この3点の実施方法は、前回説明した。(イ)のコンフィグは、忘れずに不揮発性メモリーに保存しておくことが基本だ。さらに不揮発性メモリーが故障したときに備えて、ターミナルソフトを使ってルーターの外部にファイルとして書き出しておくことが重要である。(ロ)の正常時のインタフェースの状態は、コマンドやルーター前面にあるランプで確認できる。正常時の状態を見ておく理由は、それがわからないと、異常な状態になったときに異常かどうかを判断できないからである。これは、ルーターの負荷状態を表す(ハ)のシステムロードアベレージについても同様である。

UNIVERGE IX2105の場合は「show tech-support」コマンドの活用も推奨したい。show tech-supportは、エラーログを表示する「show error-log」、不揮発性メモリーにあるコンフィグを表示する「show startup-config」、インタフェースの状態を表示する「show interfaces detail」、システムロードアベレージおよびその履歴を表示する「show utilization/show utilization history」――など、状態表示コマンドの実行結果をまとめて表示することができる(**図7**)。今回紹介したshow ipsec saコマンドとshow ike saコマンドの実行結果も、表示には含まれている。

故障の予防という観点からは、ルーターの設置方法を確認することをお勧めする。放熱の妨げになるような設置方法は、トラブルの発生原因になりかねない。UNIVERGE IX2105には、縦置きキットが標準添付されている(**写真1**)。これを使うと、狭いスペースに設置しても周囲にある程度の空間を設けられ、上に重ね置きされる心配もなくなるので温度上昇を抑制できる。温度環境がよければ、より長く安定的に稼働することにつながる。

写真1 UNIVERGE IX2105の縦置きキット
UNIVERGE IX2105では、縦置きキットが標準で添付されている。周囲に空間を確保し、温度上昇を抑制することができるため、使用することを推奨する。

▼表示することができる
今回紹介したshow logging コマンドを除く。