IRAS Ⅱ

（IPsec Remote Access Service Ⅱ）

お客様調査マニュアル

コマンドライン調査版

KDDI株式会社

はじめに

IRASⅡ（IPsec Remote Access ServiceⅡ）は、インターネット暗号化技術により、お客様ネットワークにセキュアなリモートアクセス環境を提供いたします。IRASⅡハードウェアクライアントではCisco Systems の IOS ルータ機能を利用します。

本資料は、設定マニュアルに基づき設定したが、接続できない場合、過去接続はできたが、繋がらなくなってしまった場合に参照いただくことで設定不具合箇所、環境不具合箇所の特定をする為の資料です。本資料を参照する場合、ハードウェアクライアント設定マニュアルと合わせて参照下さい。

KDDI TSC においては、お客様宅内設備（インターネット接続環境やファイアウォール/ルータ）等構成が不明確になっております。お手数ですが本マニュアルに基づき、お客様環境における不具合箇所を特定いただいた上で障害申告いただけますようお願いいたします。

本マニュアルに記載のある内容は、接続状態確認の簡易マニュアルであり、Cisco IOS ルータおよび Cisco SDM のすべての機能を説明するものではありません。

Cisco IOS ルータの詳細については、Cisco Systems の web サイトをご確認下さい。(http://www.cisco.com)

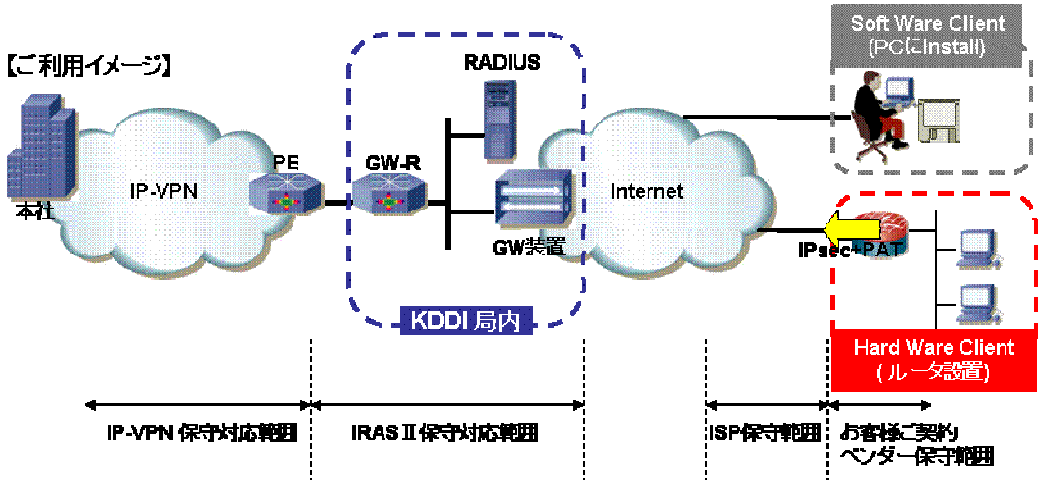
本マニュアルにて設定した内容は、お客様機器へのセキュリティを確実に保証するものではありません。必要に応じてセキュリティ設定を追加いただくようお願いいたします。

本マニュアルの内容は、改善等のため予告無く変更する場合がございますので予めご了承下さい。

第1章　IRASⅡ保守対応について

1. IRASⅡサービス保守範囲について

- IRASⅡサービスでは、ご利用いただくISPに制限はございません。
- KDDI テクニカルサービスセンター(TSC)の IRASⅡ窓口における保守対応範囲は以下の通り IRASⅡサービス保守対応範囲に限定となります。IP-VPN 等 NW サービス側については、別の担当による調査が行われます。



- KDDI TSC IRASⅡ担当窓口では、各 ISP サービスの接続状況を調査することはできません。
- **<u>サービス保守上、設定情報の取得や log 取得をご依頼させていただく場合がありますが、取得内容の分析にはお時間をいただく場合があります。</u>**

2. ハードウェアクライアントの保守対応について

- KDDI TSC IRASⅡ窓口では、ハードウェアクライアント(宅内機器)の保守手配や障害切り分けはできません。お客様ご自身での回線状態切り分けを実施いただくか、ご契約ベンダー様による切り分け／保守対応をいただくことになります。次章より記載のある方法にてお客様による状態把握をお願いいたします。
- KDDI TSC IRASⅡ窓口では、設定内容(設定上必要となる項目)確認／読み合せ程度は可能ですが、内容詳細についてのサポートについては、ご対応できません。

3. 切り分け準備

IRASⅡハードウェアクライアントとして利用するルータの情報確認方法は、いくつかの方法があります。本資料においては、コマンドライン(console)からの方法をご説明いたします。

① PC の用意

※ RS232C シリアルポートを有した PC を用意します。

※ 近年のノート PC は RS232C ポートが無い物があります。USB ポート⇔RS232C ポートへ変換するケーブルが市販されておりますのでご用意下さい。

- 変換ケーブルは、COMポートとしてPCに認識されます。(通常ドライバが必要です。)

※ ケーブルの準備ができない場合は、telnet 等での作業をお願いいたします。

※ PC にターミナルソフト(ハイパーターミナル(Windows 標準)/teraterm(フリーソフト)等)をインストールしてください。

※ 本資料では teraterm を利用しています。

※ PC 上 USB⇔RS232C 変換ケーブルが COM ポートとして認識されますが、ご利用 PC の環境によりターミナルソフトが認識できない COM ポート番号となる場合があります。その際は、ターミナルソフトの設定を変更いただき認識可能とするか、認識された COM ポートの割当を変更いただく必要があります。本作業による PC への影響はお客様責任となります。

② PC とルータの接続

- ルータと同梱されている設定用ケーブル(通常 水色)の RJ45 インターフェース側をルータ側の console と表記のあるポートへ、RS232C インターフェース側を PC の RS232C ポートに接続します。
- ターミナルソフトウェアのポート設定は、以下とします。

速度:	**9600bps**
データビット:	**8**
パリティ:	**無**
ストップビット:	**1**
フローコントロール:	**無**

第2章　開通時切り分け

1. 【 想定要因 】

お客様が、ルータを設置される際に開通確認を実施いただくことになりますが、確認時点で接続ができない場合、以下の点での不具合が考えられます。

- インターネット接続環境
  - インターネット接続(環境)の不備
  - ルータ／ファイアウォール設定不備／不足
- ハードウェアクライアント用ルータ設定
  - ファイアウォール設定の間違い
  - GW アドレス指定間違い
  - Suffix(Group Key)間違い
  - Preshared-Key 設定間違い
  - 接続アカウント(ユーザ名／パスワード)の設定間違い／重複

2. 【 確認方法 】

各種確認をいただく前に、ケーブルや接続用機器(ルータや Hub 等)の電源状態／ランプ状態等をご確認下さい。正常な接続がされているかをまず、目視にて確認いただくようお願いいたします。また、状態確認の為に利用するコマンドは特権モード(enable)でなければ入力できない物もありますので特権モードとして操作してください。

- インターネット接続環境の調査
  - インターネット接続(環境)の不備

  ※ IRAS Ⅱをご利用いただく上で ISP に制限はございませんが、Proxy サーバ経由で接続される ISP のご利用はできません。

【 コマンドラインからのインターネット状態確認 】

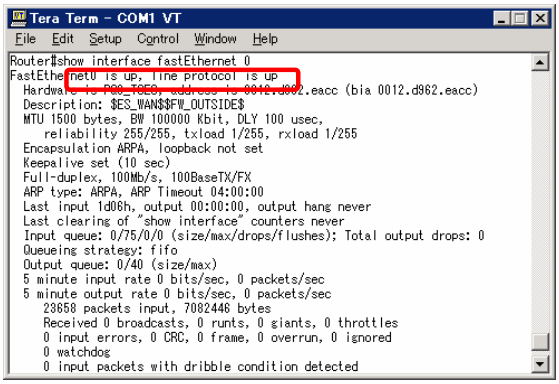
ファイアウォール機能(アクセスリスト)において ping(icmp echo/echo reply)の疎通を確保していない場合は、有効としていただく必要性があります。)

console からルータにログインします。ログイン後以下のコマンドを入力下さい。

インターネットへの出口となるインターフェースの物理的な接続状態を確認します。

“show interfaces fastethernet 4”

インターネットへの出口となる物理インターフェースの状態確認

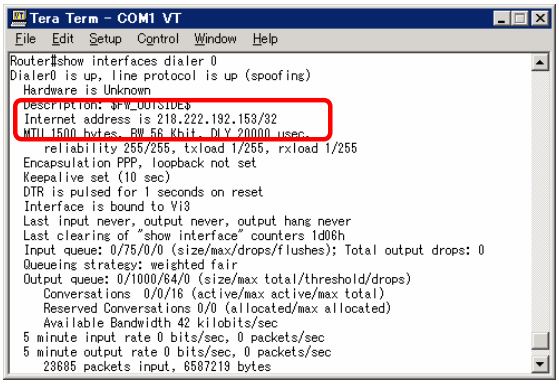


コマンド入力後次の行に UP/UP となっていることを確認します。
左図は PPPoE 利用の場合の表記の為 IP アドレス情報がありませんが、IP アドレス情報を確認します。

※ PPPoE を利用している場合

“show interfaces dialer **”

PPPoE 接続を利用している場合の出口の論理インターフェース確認

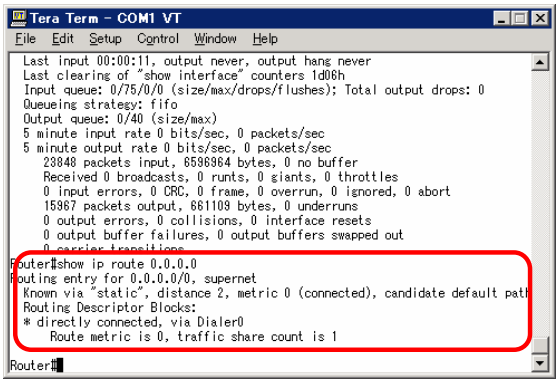


コマンド入力後、IP アドレスが取得できているかを確認します。

インターネットへ接続されているポート状態が正常であった場合、GW 装置までのルーティング状態を確認します。

“show ip route 0.0.0.0”

インターネット側へのルーティングの確認

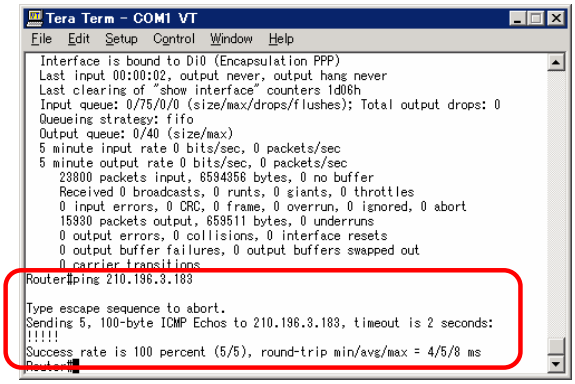


コマンド入力後、インターネットへアクセスする為のルートがあることを確認します。また想定している出力インターフェースを向いていることを確認します。

次にインターネット上との通信が本当に可能となっているのかを確認します。

“ping *.*.*.*”

インターネット上との通信可否の確認



Ping “IP アドレス”を入力します。ping に応答する IP アドレスを入力下さい。
正常に応答がある事を確認します。
GW 装置は ping 応答しませんので別アドレスを宛先としてください。

[インターネット接続状態が正常ではなかった場合]

前述までの確認を行った結果正常な状態ではなかった場合それぞれの項目を調査してください。

“show interfaces fastethernet 4”が UP/UP となっていなかった場合

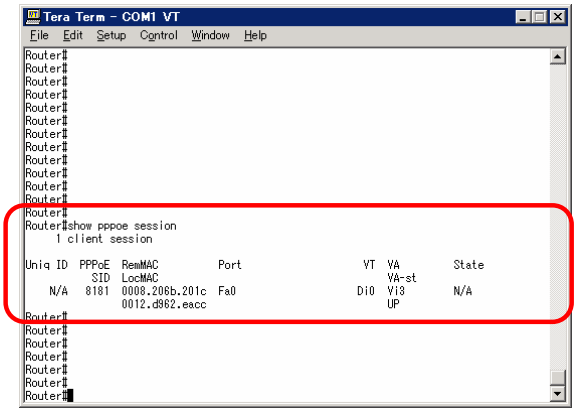
- “administratively down”の表示が存在した場合・・・ポートが shutdown 状態です。設定モードに移行し”no shutdown”コマンドを入力して保存してください。
- “FastEthernet4 is up, line protocol is down”の場合・・・ケーブル不良や対向装置のポート不良/自装置のポート不良の可能性があります。繋ぎ変え等の作業を実施してください。

“show interfaces dialer **”でアドレスが付与されていない場合

- PPPoE の ID/Password が間違っている可能性があります。

※ 固定 IP アドレスの割当をされている場合は、PPPoE 接続状態を確認する必要がある為以下のコマンドを入力します。

“show pppoe session”



PPPoE セッション情報を確認可能です。UP となっていない場合、PPPoE 接続に問題がある可能性があります。(回線不具合/設定間違いを含む)

“show ip route 0.0.0.0”で”% Network not in table”となった場合

- 想定している出力インターフェースからパケットが送信されるようルーティングテーブルを入力する必要性があります。

“ping *.*.*.*”が 100% loss となった場合

- Next Hop として指定しているアドレスへの疎通ができない可能性があります。
- ファイアウォール(アクセスリスト)等で ping の疎通が確保されていない可能性があります。
- インターネット接続と IRASⅡ接続用ルータが別装置の場合、他の装置側の設定を確認する必要性があります。

➢ ルータ／ファイアウォール設定の不備／不足

IRASⅡ接続を実施する上でルータやファイアウォールなどの配下から接続されている場合、特定プロトコルの疎通を確保する必要性があります。非 NAT 環境下では ESP パケットを疎通させる必要性があります。ルータやファイアウォールにて以下のプロトコル疎通が許可されていることを確認してください。

【 LAN ⇒ WAN 方向 】
アドレス：
Src=ハードウェアクライアント WAN 側アドレス
Dst=“GW アドレス”
プロトコル/ポート:
UDP Src Port:不定 Dst Port:500
UDP Src Port:不定 Dst Port :4500
ESP パケット

※ ESP とは、”Encapsulation Security Payload”と略で IPsec による暗号化されたパケットを表します。

【 WAN ⇒ LAN 方向 】
アドレス：
Src=GW アドレス
Dst=ハードウェアクライアント WAN 側アドレス
プロトコル/ポート:
UDP Src Port:500 Dst Port:不定
UDP Src Port:4500 Dst Port :不定
ESP パケット

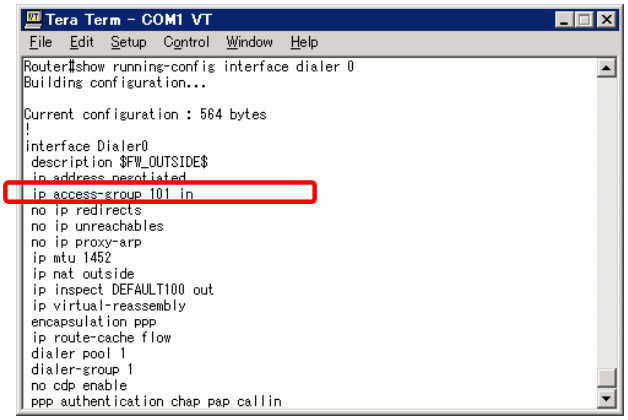
- ハードウェアクライアント用ルータ設定の調査

  インターネット接続状態を確認後、接続状態に問題が無かった場合、ハードウェアクライアントとして利用するルータ設定の不備が考えられます。IRAS Ⅱとの接続においては、KDDI より通知する、開通案内の情報を間違いなく設定すると共に、IRAS Ⅱ接続用の前述特定プロトコルのパケットの疎通を確保する必要性があります。

  ➢ ファイアウォール(アクセスルール)設定の間違い

  実際のアクセスルール設定内容を以下の手順で確認することができます。

  “show running-config interface XXX **”(XXX **には LAN 側/WAN 側のインターフェース名を入力します。)



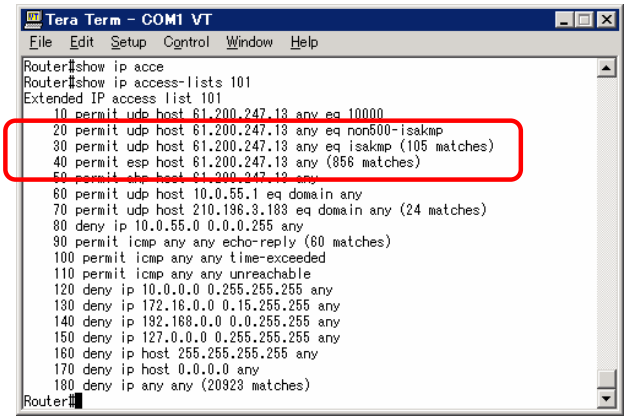
コマンドを入力し、”ip access-groupxx”の記載があるかを確認します。in/outの方向記載がありますが両方有る場合、それぞれを確認します。

※方向記載=in　当該インターフェースに入ってくるパケットに対するルール

※方向記載=out当該インターフェースから出ていくパケットに対するルール

次にルールの詳細を確認します。

“show ip access-list XX”



コマンド入力後アクセスリストの詳細が表示されます。IRAS Ⅱ接続で使用されるプロトコルの疎通が確保されていることを確認してください。

アウトバウンドトラフィック/インバウンドトラフィックにて疎通が確保されていることを確

認してください。

【アウトバウンドトラフィック】

LAN 側から発信され、WAN へ送出されるトラフィックに対するルールとなります。LAN 側インターフェースの in のルール/WAN 側インターフェースの out のルールを確認します。

[LAN 側インターフェースで受信するパケットの許可]

少なくとも IRAS Ⅱ で接続する宛先へのパケットを受信する必要性があります。

[WAN 側インターフェースで送信するパケットの許可]

少なくとも IRAS Ⅱ 接続用の IPsec 関連パケットを送信する必要性があります。

【インバウンドトラフィック】

WAN 側から到着し、LAN へ送出されるトラフィックに対するルールとなります。LAN 側インターフェースの out のルール/WAN 側インターフェースの in のルールを確認します。

[WAN 側インターフェースで受信するパケットの許可]

少なくとも IRAS Ⅱ 接続用の IPsec 関連パケットを受信する必要性があります。

[LAN 側インターフェースで送信するパケットの許可]

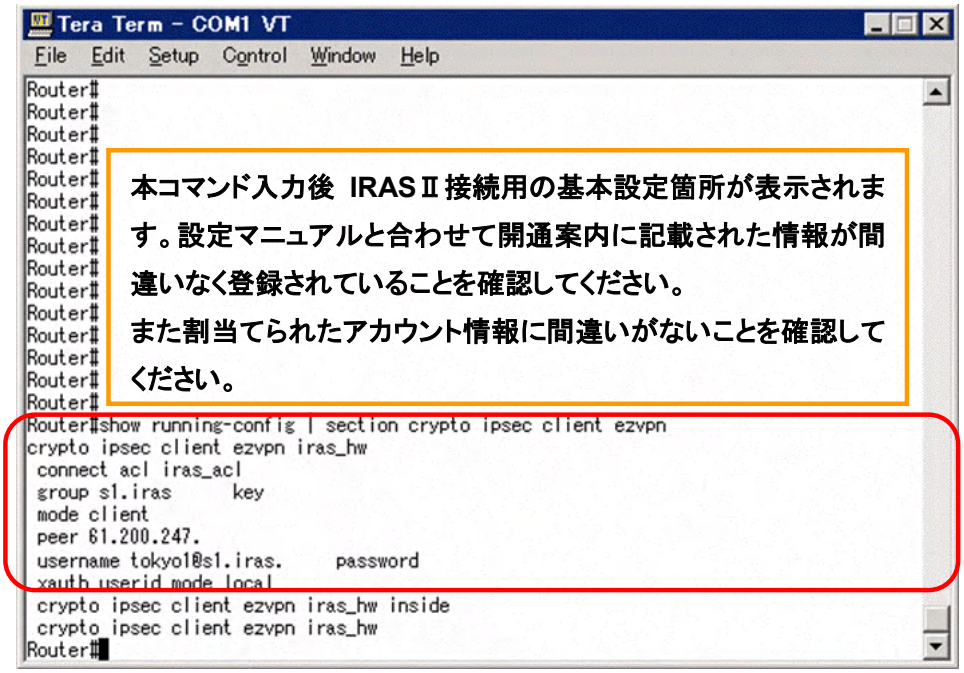
少なくとも IRAS Ⅱ で接続するクライアントへのパケットを送信する必要性があります。

- IRAS Ⅱ 接続設定の不備

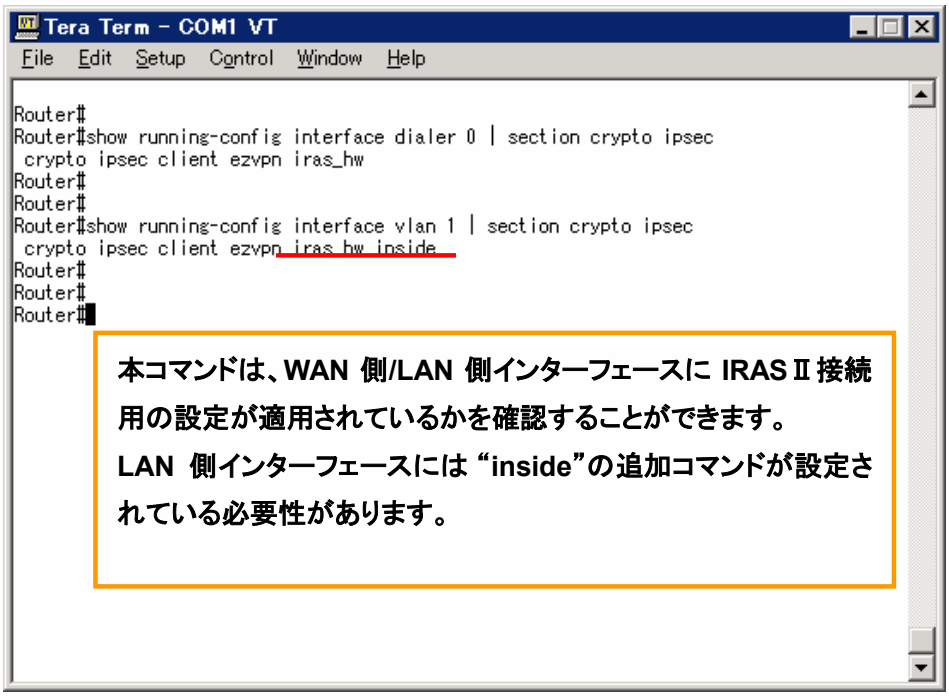
IRAS Ⅱ ご契約時にお渡しする開通案内に記載された内容と該当拠点に割当てられたアカウント情報に間違いがないかを確認いただくと共に、ルータ LAN 側/WAN 側に正しく IRAS Ⅱ 接続用設定が適用されていることを確認する必要性があります。

下記コマンドを入力することで設定情報を確認することができます。

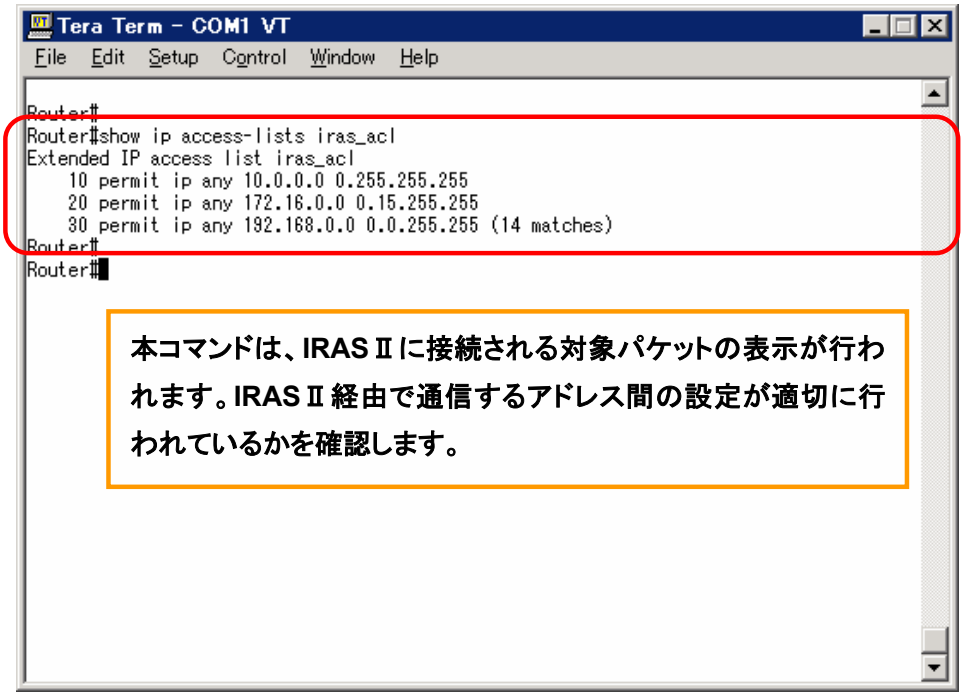
“show running-config | section crypto ipsec client ezvpn”



“show running-config interface “インターフェース名” | section crypto ipsec”



“show ip access-list iras_acl”



本コマンドは、IRASⅡに接続される対象パケットの表示が行われます。IRASⅡ経由で通信するアドレス間の設定が適切に行われているかを確認します。

第3章　利用開始後の障害切り分け

1. 【 想定要因 】

お客様がご利用開始後に通信ができない状態となった場合、以下の不具合が考えられます。

- インターネット接続環境
  - ご利用中にインターネット接続環境に障害が発生した可能性
  - ルータやファイアウォールの故障や交換による設定漏れの可能性
- ハードウェアクライアント用ルータ故障
  - ルータファーム(Cisco IOS)のバグ等による不具合の可能性
  - ハード故障

2. 【 確認方法 】

各種確認をいただく前に、ケーブルや接続用機器(ルータや Hub 等)の電源状態／ランプ状態等をご確認下さい。正常な接続がされているかをまず、目視にて確認いただくようお願いいたします。

- インターネット接続環境の調査
  - インターネット接続環境の障害

    第２章 2.に記載のある【 コマンドラインによるインターネット状態確認 】を実施でインターネット状態を確認することができます。

    インターネット接続状態の詳細については、ご契約の ISP へご確認下さい。
  - ルータやファイアウォールの故障

    設定変更の有無／交換作業やバージョンアップ作業等の有無を確認いただくか、ルータ／ファイアウォール保守ベンダーへ連絡し切り分け作業を実施してください。
- ハードウェアクライアント用ルータ故障の調査

  インターネット接続環境に問題が無い場合、ハードウェアクライアント用ルータ故障およびルータ周辺接続装置の故障が想定されます。ケーブルや接続機器の電源状態／ランプ状態に問題が無ければ以下想定を考慮し対処を実施してください。
  - ルータファーム(Cisco IOS)のバグ等による不具合の可能性

    KDDI にてハードウェアクライアント用として選定しているルータは、IRAS Ⅱ 接続に関わる不具合が発生しないことを前提としております。お客様がご利用になられる機能によっては、ソフトウェア不具合が内在している可能性があります。

ソフトウェア不具合は、ルータ再起動等で解消される場合がありますのでルータ電源の off/on を実施し、再度接続を実施してください。(再起動後 5 分程度通信ができない場合があります。)

- ハード故障の可能性

ハード故障のうち、ポート不良等は、接続に利用しているケーブルの接続変更等を行うことで解消される場合がありますが、ルータ再起動を実施しても解消されない場合、保守ベンダーへご連絡いただき機器交換を実施してください。

第4章　KDDI へのエスカレーション調査

上記までの確認を実施した結果、ISP 接続、ISP 接続機器、ファイアウォール、ハードウェアクライアント用ルータすべてに不具合が発見できない場合、KDDI TSC IRASⅡ窓口へご連絡下さい。KDDI TSC IRASⅡ窓口では、インターネット接続状況および IRASⅡ接続設定、該当ハードウェアクライアントに割当てられた接続用アカウントをヒアリングさせていただきます。

接続用アカウントのヒアリング結果より弊社認証設備での状況を確認した上で原因特定ができなかった場合、ルータ log を取得いただくお願いをいたします。

- log 取得について

  KDDI 調査を行う上で必要とする log を取得する場合もコマンドラインからの取得をお願いすることになります。取得いただきました log は KDDI TSC IRASⅡ窓口までメールでご送付いただくことになります。log 解析にはお時間を頂戴いたします。(数日程度)

- log 取得方法

  ルータの Console ポートにルータと同梱されている console ケーブルを接続いただくか、telnet から接続いただく必要性があります。

※　console ケーブルを利用した log 取得には、RS-232C シリアルポートが必要となります。

※　近年発売されているノート／ラップトップ型 PC では、RS-232C シリアルポートが存在しない場合があります。その場合 USB⇔RS-232C ポート変換ケーブルをご用意いただく必要があります。

※　通常 RS-232C 変換ケーブルは、ドライバが必要です。

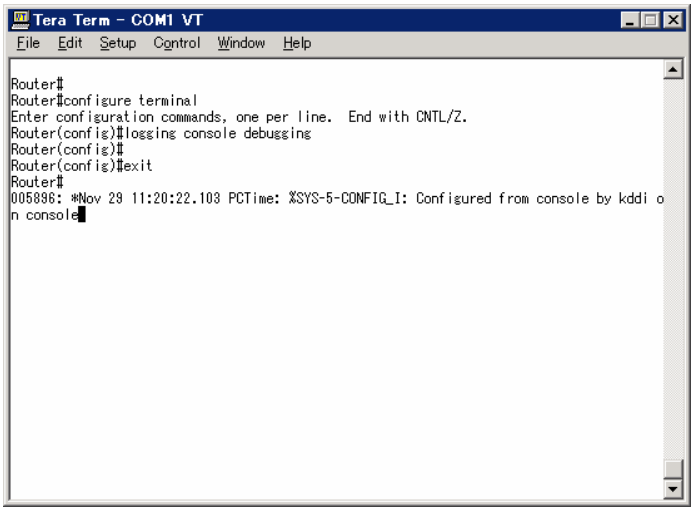
本資料では、teraterm を利用し console にて log 取得する方法を記載いたします。

- log 出力準備

ルータへのログイン後,設定モードへ移行し、console 画面上に log を出力する為の設定を行います。

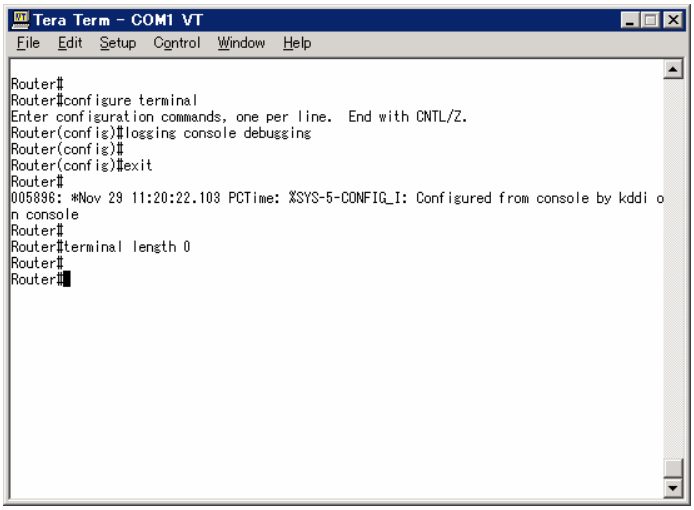
“configure terminal”と入力し Enter を押し、設定モードへ移行します。

“logging console debugging”と入力し Enter を押し、cosnole 画面上への log 出力を許可します。入力後”exit”と入力し、設定モードから抜けます。

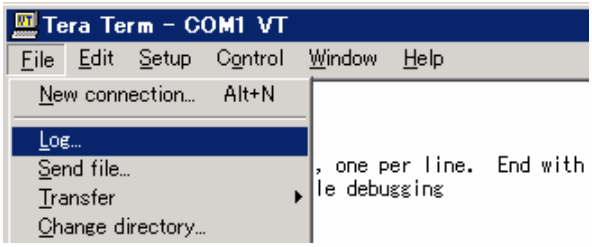


次に、以下のコマンドを入力します。

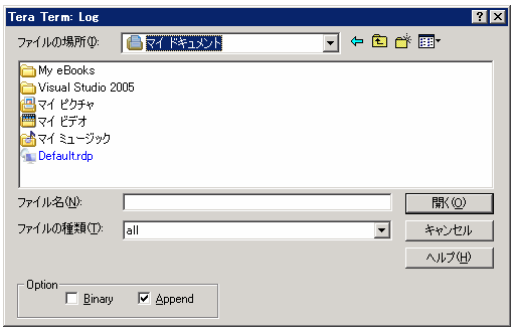
“terminal length 0”

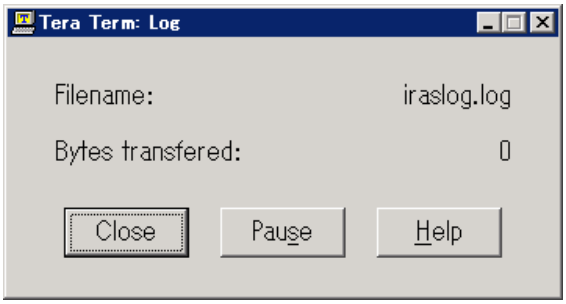


コマンド入力後以下の操作を行い、telnet 画面出力結果をテキストファイルに保存します。



File⇒log を選択し、適当な場所とファイル名を作成し開くをクリックします。
※テキストファイルで閲覧できる形式の為、”.txt”や”.log”などの拡張子をご利用下さい。





保存するファイルを規定すると左図のようなウィンドウが立ち上がり log 取得状態となります。

ここまで完了するとルータからの出力情報がテキストファイルに随時保存されます。

[IPsec 専用 log の取得]

続いて以下のコマンドを入力します。

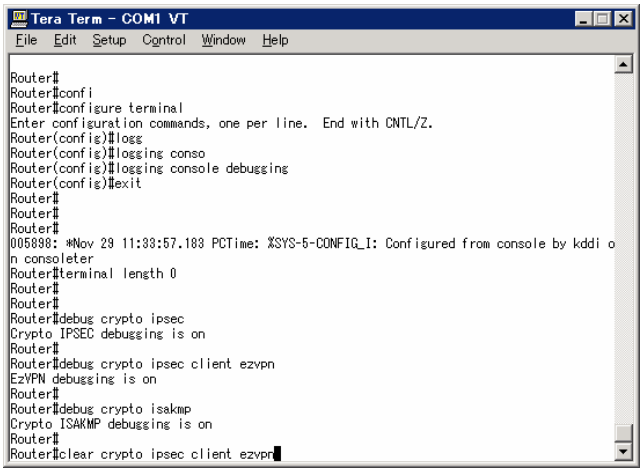
“debug crypto ipsec”

“debug crypto ipsec client ezvpn ”

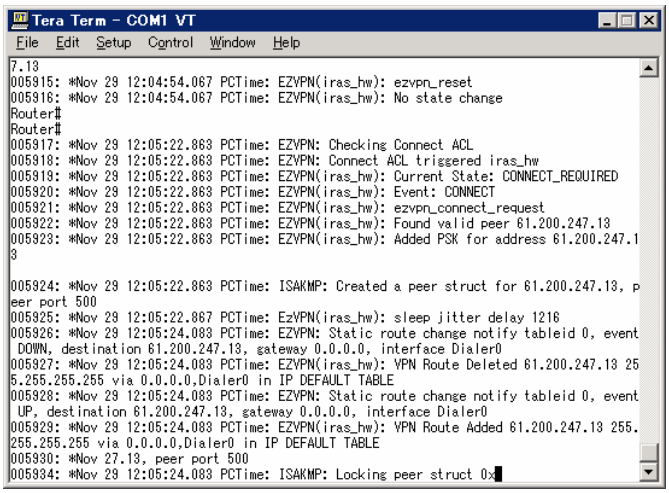
“debug crypto isakmp”

“clear crypto ipsec client ezvpn”

各コマンドを入力することによりメッセージがルータより返ってきます。



IRAS Ⅱ へ接続する対象のパケットが LAN 側からルータへ到着している場合、以下のように画面上にテキスト表示がされます。パケットが到着していない場合は、何の表示もされない為、LAN 上の PC 等から IRAS Ⅱ 接続対象へ ping を送出してください。

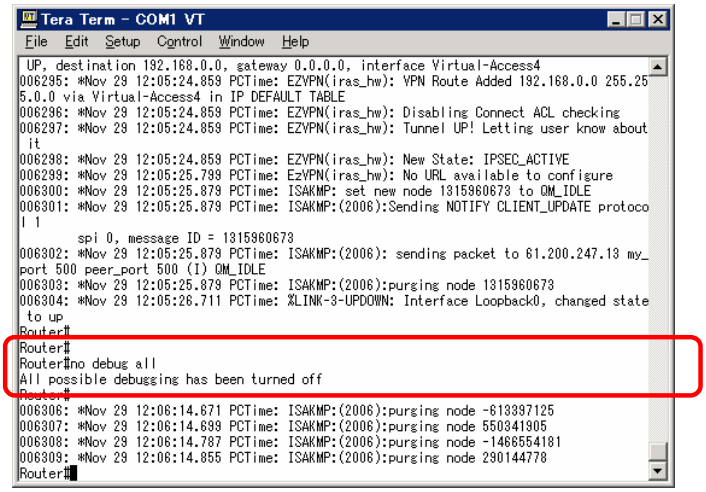


3 分程度放置し以下のコマンドを入力してください。

“no debug all”

画面上の出力が停止します。

※”no debug all”と入力後もテキスト表示が止まらない場合、数回同じコマンドを入力いただくようお願いいたします。



[ルータ情報の取得]

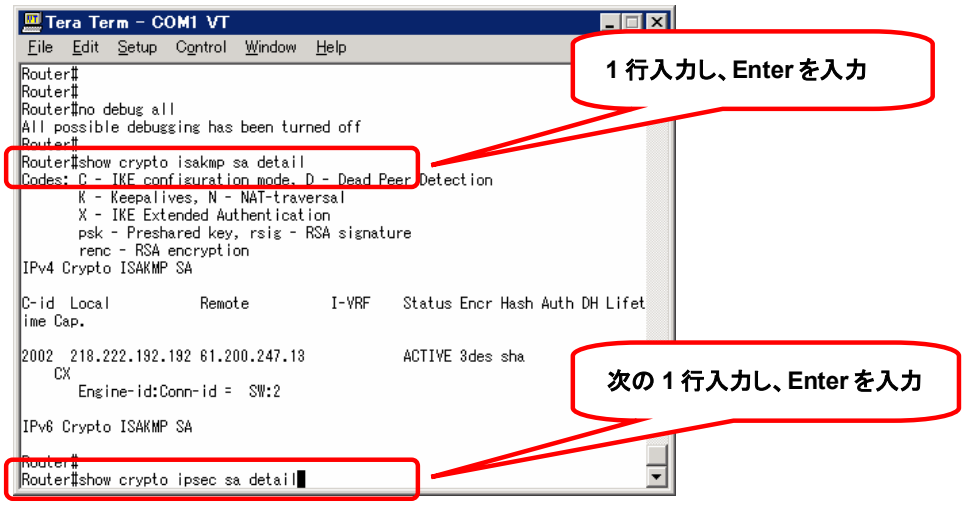
ルータの情報を出力する為以下のコマンドを入力します。

“show crypto isakmp sa detail”

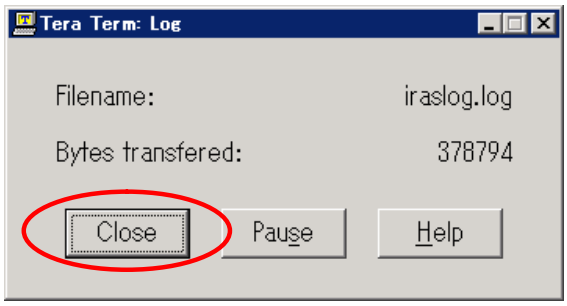
“show crypto ipsec sa detail”

“show tech-support”

それぞれのコマンド入力後 Enter を押すことでテキストファイルが出力されます。



画面上の出力を停止した後、テキストのキャプチャを停止します。



Log 出力時に表示されたウィンドウの close ボタンをクリックしキャプチャを停止します。

テキストキャプチャの停止が完了したら、以下のコマンドを入力しルータからログアウトしてください。

“exit”

ルータからログアウトが完了したらハイパーターミナルを終了し、保存していたファイルを KDDI TSC IRAS Ⅱ 窓口よりお知らせするメールアドレス宛にご送付下さい。

本マニュアルお問い合わせにつきましては、弊社営業担当までご連絡下さい。

IRASⅡ（IPsec Remote Access Service　Ⅱ）
ハードウェアクライアントお客様調査マニュアル コマンドライン調査版

作成日:2008 年 3 月 3 日　　第 1.0 版
作成者:KDDI 株式会社

※　本マニュアルの内容は改善のため、予告なく変更する可能性があります。