ezTCP series

仮想ＣＯＭポートソフトウェア

ＴＣＰ－ＶＳＰ

取り扱い説明書

5.4 版

ALPHA PROJECT

ご使用になる前に

このたびはＴＣＰ－ＶＳＰをお買い上げいただき誠にありがとうございます。
本製品をご活用いただくために、本マニュアルをよくお読みください。
今後共、弊社製品をご愛顧賜りますよう宜しくお願いいたします。

梱包内容

本製品は、下記の品より構成されております。梱包内容をご確認のうえ、万が一、不足しているものがあれば、お買い上げ販売店までご連絡ください。

梱包内容

●ＴＣＰ－ＶＳＰ　ＣＤ－ＲＯＭ	１枚
●マニュアル・サンプルプログラムのダウンロード・保証のご案内	１枚

■本製品の内容及び仕様は予告なしに変更されることがありますのでご了承ください。

取り扱い上の注意

●本製品を宇宙、航空、医療、原子力、運輸、交通、各種安全装置など人命、事故に関わる特別な品質、信頼性が要求される用途でのご使用はご遠慮ください。

本製品は、使用するアプリケーションや、動作環境（他にインストールされているアプリケーションの影響 等）によっては正常に機能しない場合があります。その場合は、アプリケーションの修正、または、動作環境の変更により対応して下さい。

保証

■本製品は万全の注意を払って作成されていますが、万一ディスクの不良等があった場合、お買い上げいただいた販売店へ保証書を添えてご返却ください。
■万が一、本製品を使用して事故または損失が発生した場合、弊社では一切その責を負いません。
■保証内容、免責等につきましては、添付の保証書をご覧ください。
■本製品を仕様範囲を超える条件において使用された場合については、動作は保証されません。
■製品を改造した場合、保証は一切適用されません。
■他社製品との相性問題は保証いたしません。

目　次

■製品サポートのご案内　　■エンジニアリングサービスのご案内

1．製品概要

１．１　概要

ＴＣＰ－ＶＳＰは、ＴＣＰ（ＵＤＰ）ポートを仮想ＣＯＭポートとして扱えるＷｉｎｄｏｗｓアプリケーションです。

１．２　特徴

１）ソケット通信プログラムの作成が不要

アプリケーション開発者は、ＣＯＭポートの通信と同じようにＴＣＰ（ＵＤＰ）通信が行えますので、ＴＣＰ（ＵＤＰ）通信に必要なソケット通信のプログラミング知識は必要ありません。

２）　既存のＲＳ２３２通信システムをＬＡＮ・ＷＡＮ環境に移行可能

弊社製品「ｅｚＴＣＰ」シリーズと組み合わせて利用することにより、既存のＲＳ２３２通信システムをＬＡＮ・ＷＡＮ環境に簡単に移行することができます。

３）最大 256 個の仮想ＣＯＭポートの作成／通信が可能

最大で 256 個(COM1～COM256)の仮想ＣＯＭポートをサポートしています。
※ハードウェアリソースですでに割り当てられているＣＯＭポートに仮想ＣＯＭポートを割り当てることはできません。

４）ＴＣＰポート（サーバ，クライアント），ＵＤＰポートに対応

ＴＣＰ／ＩＰ、ＵＤＰに対応しており、ＴＣＰ／ＩＰではサーバ、クライアントが選択できます。
仮想ＣＯＭポート毎に設定できますので、ＴＣＰ（サーバ）、ＴＣＰ（クライアント）、ＵＤＰを混在させて動作させることもできます。

５）ＳＳＬ／ＴＬＳによる暗号化に対応

ＳＳＬ／ＴＬＳに対応していますので、通信データの暗号化により、安全にデータの送受信ができます。

６）ログイン機能に対応

ユーザ名、パスワード認証によるログイン機能をサポートしていますので、不正な接続を防ぐことができます。

７）Ｔｅｌｎｅｔプロトコル対応

Ｔｅｌｎｅｔプロトコル（サーバモード、クライアントモード）に対応しています。

８）接続維持機能

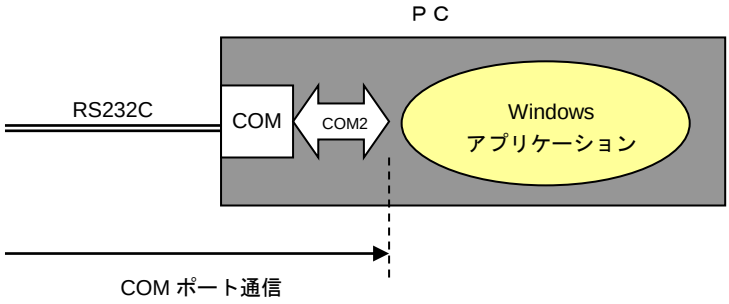
ＴＣＰ／ＩＰの接続が何らかの問題により切断された場合、自動的に再接続することができます。また、切断検出のための、キープアライブをサポートしています。

２．機能説明

２．１　動作概要

ＴＣＰ－ＶＳＰは、ネットワーク上のＴＣＰ（ＵＤＰ）ポートを仮想ＣＯＭポート（シリアルポート）にリダイレクトします。
動作イメージを図 2.1.1 に示します。
ＴＣＰ－ＶＳＰの機能により、ＷｉｎｄｏｗｓアプリケーションからはＴＣＰ（ＵＤＰ）ポートを標準のＣＯＭポートと同じようにアクセスすることができます。

■一般的な COM ポートを使った通信アプリケーションの動作イメージ



■ＴＣＰ－ＶＳＰ＋アプリケーションの動作イメージ

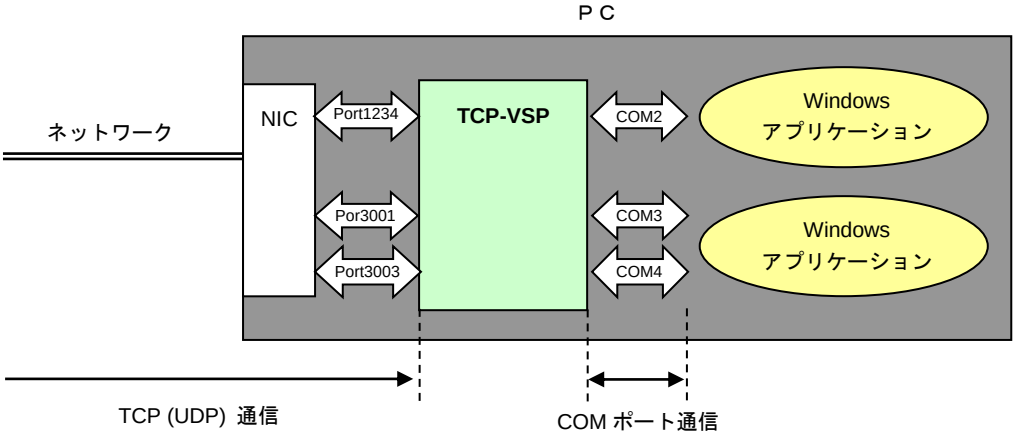


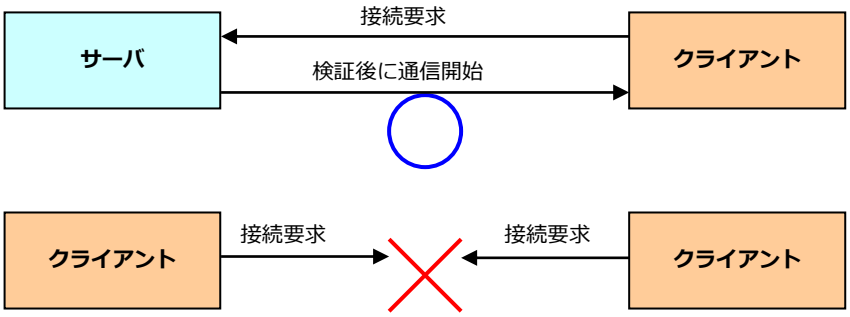
図 2.1.1　ＴＣＰ－ＶＳＰの動作イメージ

２．２　動作モード

ＴＣＰ－ＶＳＰは、ＴＣＰモードとＵＤＰモードの２つの動作モードが用意されています。
以降に、それぞれの動作について説明します。

２．２．１　ＴＣＰモード

ＴＣＰは、コネクション型の通信であり、最初に接続を確立してから通信を行います。
２点間で通信を行う場合には、一方がサーバでもう一方はクライアントとなります。このサーバとクライアントの違いを、簡単に説明すると、クライアントはサーバに接続要求を出す側であり、サーバはクライアントからの接続要求を待つ側であるということだけです。接続が確立したあとは双方向で通信が可能です。
ＴＣＰ－ＶＳＰは、仮想ＣＯＭポート毎にサーバとクライアントを個々に設定ができるため、通信相手がサーバでもクライアントでも通信することが可能となっております。
以上のことから、ＴＣＰモードは、データの信頼性を重視するアプリケーションに適しているといえます。



※ 必ず一方がサーバで、もう一方がクライアントでないと接続を確立できない。

図 2.2.1　ＴＣＰモードのサーバとクライアントの関係

ＴＣＰ通信の特徴

・サーバとクライアントがあり、１対１でコネクションを確立してから通信を行う。
・送受信では、エラー訂正が行われ、相手先で正しく受信できなかった場合には再送信が行われる。

２．２．２　ＵＤＰモード

ＵＤＰは、ホスト／クライアントの概念がありません。そのため、ＴＣＰのように送受信開始前に接続要求等の必要がなく、送信側からＩＰアドレスとポート番号を指定すれば相手先にデータを送信できます。ただし、ＴＣＰ通信と異なり、接続確認やエラー訂正を行わないため、データの確実性は保証されません。

また、ＵＤＰの特徴として、ブロードキャストアドレスによる送受信が可能です。
ブロードキャストとは、一つのデータを同一ネットワーク内の全機器に伝える通信で、送信先のＩＰアドレスを 255.255.255.255 にすることにより同一ネットワーク内の全機器にデータを送信します。これによりデータを一つのＵＤＰポートから一度に複数のＵＤＰポートに送信することができます。
以上のことから、ＵＤＰモードはデータの信頼性よりも、多対多の通信や、通信の高速化を重視するアプリケーションに適しているといえます。

■ＵＤＰ送受信イメージ

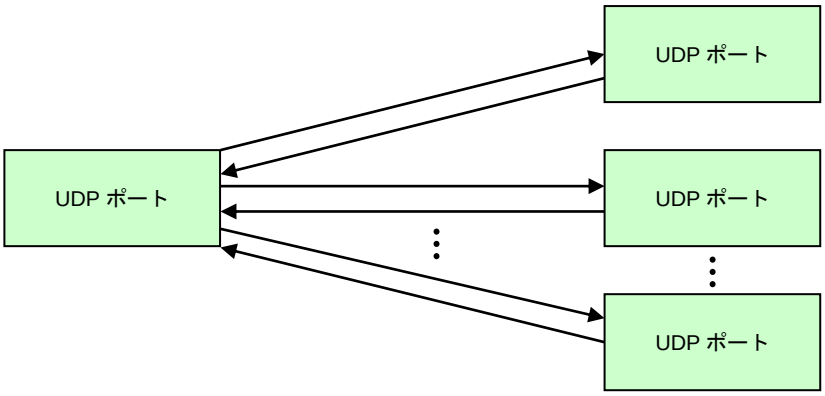


図 2.2.2　ＵＤＰ送受信イメージ

ＵＤＰ通信の特徴

・ホスト／クライアントの概念がなく、通信相手と通信開始前にコネクションを確立しない。
・データの確実性は保証されない
・ブロードキャストアドレスにより、多対多の送受信が可能。

２．３　セキュリティ機能

ＴＣＰ－ＶＳＰは、セキュリティ機能としてＳＳＬ／ＴＬＳによる暗号化とログイン認証によるアクセス制御機能が実装されています。以下に、それぞれの機能について説明します。

２．３．１　ＳＳＬ／ＴＬＳによる暗号化

一般的にネットワーク通信においては、データの盗聴、改竄、なりすまし等の不正行為が少なからず存在します。
これらの不正行為から通信データを守るために、ＴＣＰ－ＶＳＰでは、ＳＳＬ／ＴＬＳによる暗号化をサポートしています。

* SSL（Secure Socket Layer）とは、Netscape Communication 社が提案したセキュリティプロトコルで、暗号化、認証等のセキュリティ機能を提供することができるプロトコルです。その後、インターネット標準化案がまとまりＴＬＳ(Transport Layer Security)という名称で RFC2246 として公開されることになりました。ＴＣＰ－ＶＳＰでは、SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2 に対応しています。

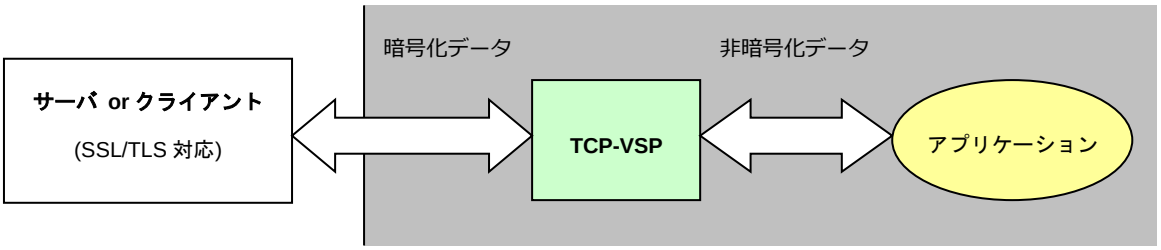


図 2.3.1　暗号化通信のイメージ

２．３．２　ログイン認証によるアクセス制限

ＴＣＰ－ＶＳＰでは、サーバモードで動作している場合に、接続時にユーザ名とパスワードによる認証を行うことができます。
この認証処理により、不正な接続を防ぐことができます。

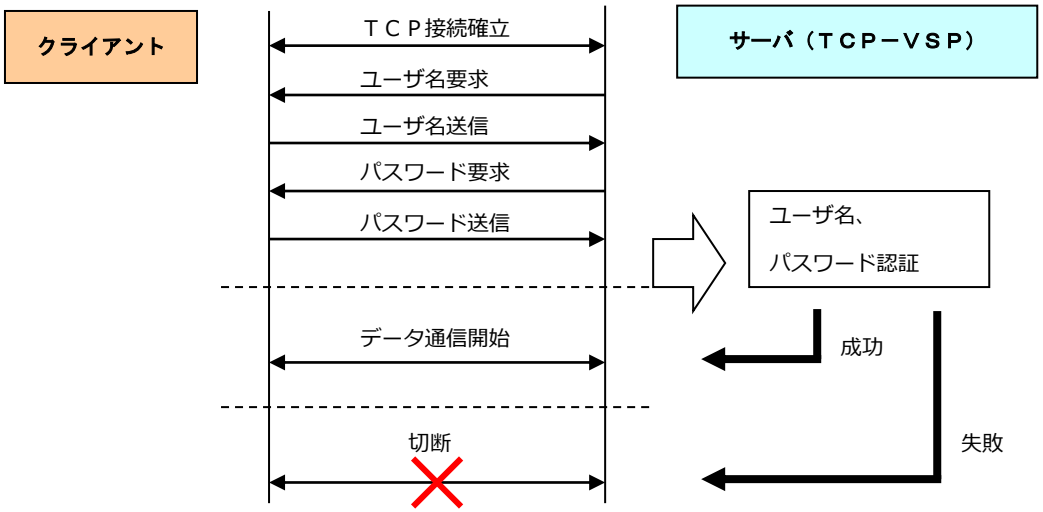


図 2.3.2　ログイン認証時の接続方法

２．４　Ｔｅｌｎｅｔ機能

ＴＣＰ－ＶＳＰは、Ｔｅｌｎｅｔプロトコルをサポートしています。
以下に、Ｔｅｌｎｅｔプロトコルの機能について説明します。

２．４．１　Ｔｅｌｎｅｔプロトコルによる通信

Ｔｅｌｎｅｔプロトコルとは、サーバとクライアント間の通信方法の１つです。
ＴＣＰ－ＶＳＰは、Ｔｅｌｎｅｔプロトコルを内部で処理するので、アプリケーションソフトは、Ｔｅｌｎｅｔプロトコルを意識せずに、ＴｅｌｎｅｔサーバやＴｅｌｎｅｔクライアントとして動作することができます。

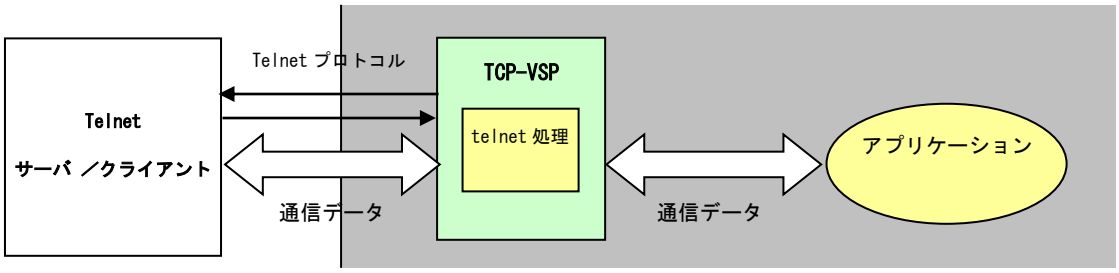


図 2.4.1　Ｔｅｌｎｅｔプロトコルの動作イメージ

２．５　接続維持機能

ＴＣＰ／ＩＰ通信は、何らかの問題によりサーバとクライアント間の通信接続が切断されてしまった場合、再度接続しないと通信はできません。
ＴＣＰ－ＶＳＰでは、再接続を自動的におこなう接続維持機能があります。本節では、その接続維持機能の説明をします。
なお、本機能はＴＣＰ／ＩＰ通信の場合のみ使用できます。ＵＤＰ通信では接続がないため使用できません。

➢シリアル通信の場合、一般的に通信相手との接続を確認して通信しないため、TCP-VSP を使用するアプリケーションは、接続が切断されてもデータを送信し続ける状況になる可能性があります。そのような状況を回避するためには接続維持機能の使用が有効です。

２．５．１　概要

ＴＣＰ－ＶＳＰの接続維持機能の動作概要を説明します。
ＴＣＰ／ＩＰ通信では、一旦通信が切断されると、そのままでは通信を回復することができません。(図 2.5.1)
ＴＣＰ－ＶＳＰで接続維持機能を有効とした場合、通信が切断されると、ＴＣＰ－ＶＳＰはＴＣＰ／ＩＰの再接続を行い、通信を回復することができます。(図 2.5.2)

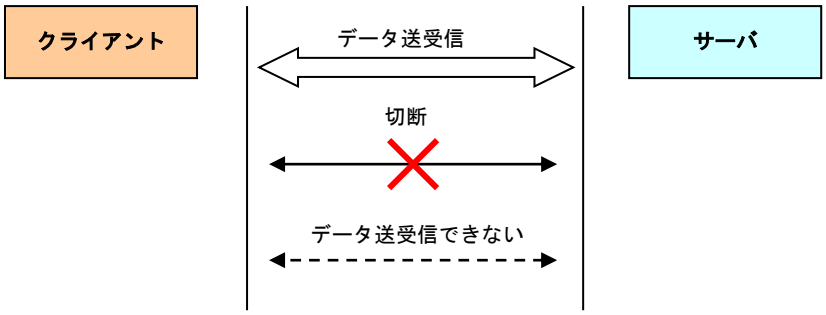


図 2.5.1　接続切断時の動作イメージ

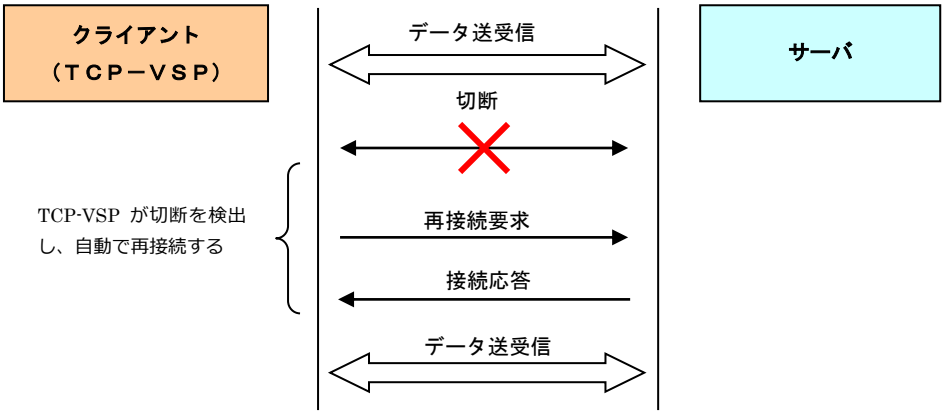


図 2.5.2　接続維持機能の動作イメージ

ＴＣＰ－ＶＳＰの接続維持機能は、主に「通信の切断検出」と「自動再接続」の２つの動作からなります。

【通信の切断検出】

ＴＣＰ－ＶＳＰは下記のいずれかに条件に該当した場合、通信が切断状態と判断します。

1. クライアントもしくはサーバが切断要求を送信し、接続先が要求を受け入れた場合。
2. クライアントもしくはサーバがデータを送信したが、接続先から応答が無かった場合。
3. クライアントもしくはサーバがキープアライブ要求を送信したが、接続先から応答が無かった場合。

【自動再接続】

自動再接続は、ＴＣＰ－ＶＳＰがＴＣＰ／ＩＰのクライアントの場合のみ有効です。
ＴＣＰ－ＶＳＰは切断状態と判断した時に、自動でサーバへ接続要求を行います。

➤切断状態から再接続されるまでの間の通信データは失われる可能性がありますのでご注意ください。

機　能		ＴＣＰ－ＶＳＰ　動作モード	
		クライアント	サーバ
切断検出	データ送信タイムアウト	常に行う	常に行う
	キープアライブ	使用可能	使用可能
自動再接続		使用可能	使用不可

表 2.5.1　ＴＣＰ－ＶＳＰの接続維持機能

２．５．２　切断検出 －データ送信タイムアウト－

ＴＣＰ／ＩＰの切断検出の１つとして、データの送信タイムアウトによる検出方法があります。
基本的にデータ送信は、以下のような接続先からの応答があって送信完了となります。

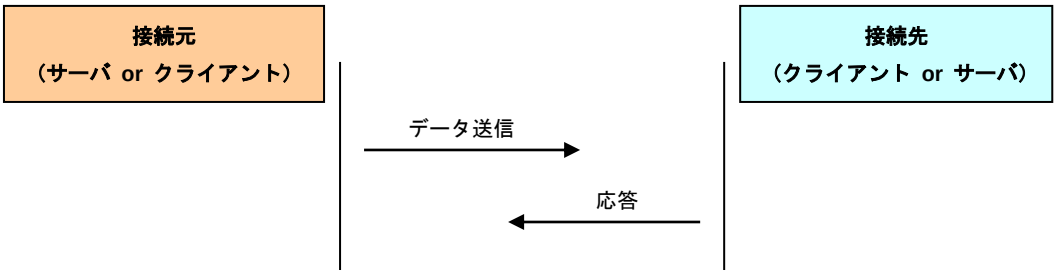


図 2.5.3　データ送信のイメージ

もし、何らかの問題により応答がなかった場合は、データの再送信を行います。
そして、特定の回数再送信を行っても応答がない場合に、送信元は切断されていると判断します。
以下に示すのが、データ送信のタイムアウトによる切断検出のイメージ図です。

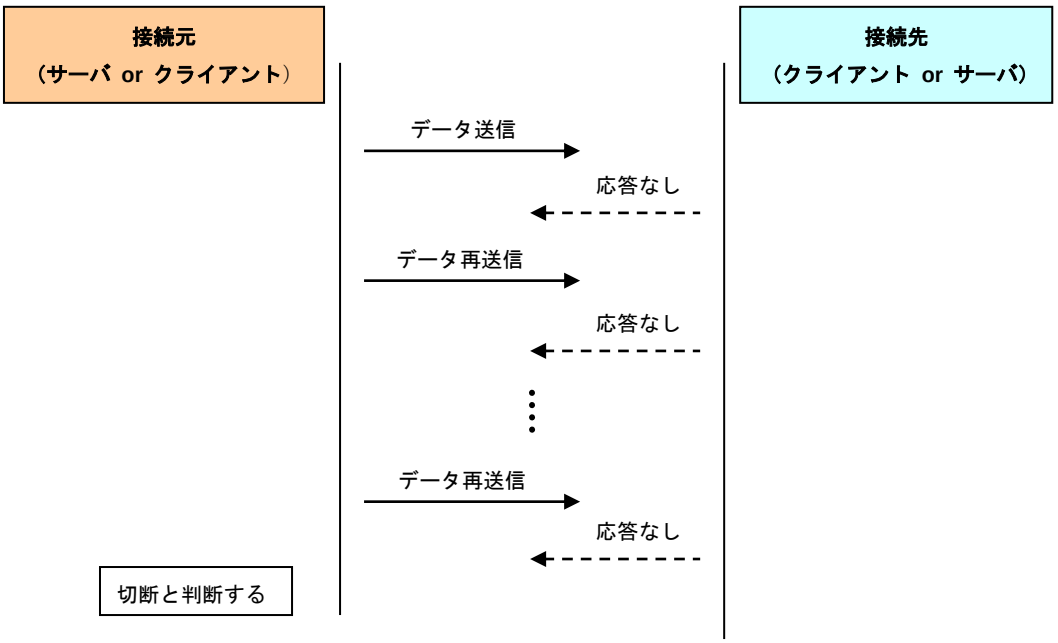


図 2.5.4　データ送信タイムアウトのイメージ

➤データ再送信時間や切断判断に関しては、ＯＳ（Ｗｉｎｄｏｗｓ）で定められている設定で行います。

２．５．３　切断検出 －キープアライブ－

キープアライブとは、ネットワーク上で接続が有効であることを確認するための通信手段です。
キープアライブの目的は主に２つあります。
１つは、この経路はまだ有効であることを接続先に伝えること。もう１つは、接続されている経路がまだ有効であるかを確認することです。
なお、キープアライブは、ＴＣＰ／ＩＰの接続間でキープアライブ要求を定期的に送信することで行います。
以下が、通信のイメージ図です。

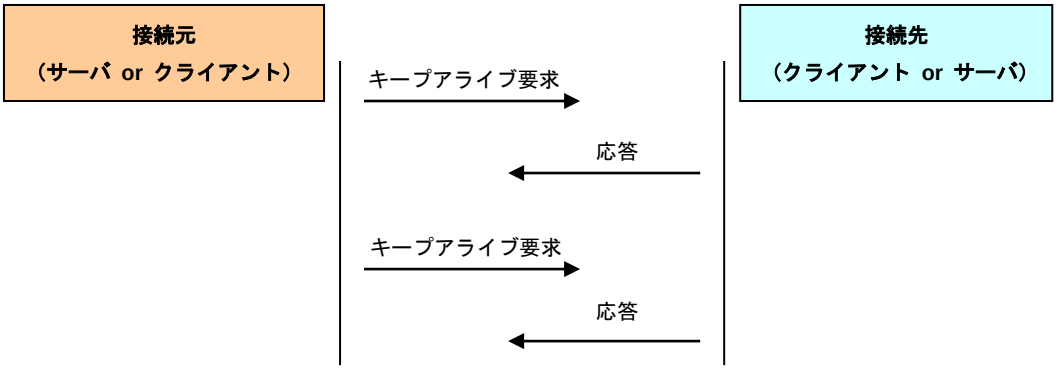


図 2.5.5　キープアライブの動作イメージ

キープアライブ要求を接続先に送ることで有効であることを伝え、接続先から応答があることで接続されている経路が有効であることが確認できます。

キープアライブによる切断検出は、キープアライブ要求に対する応答が特定の回数（TcpMaxDataRetransmissions）無かった場合に切断されていると判断します。
以下が、動作のイメージ図です。

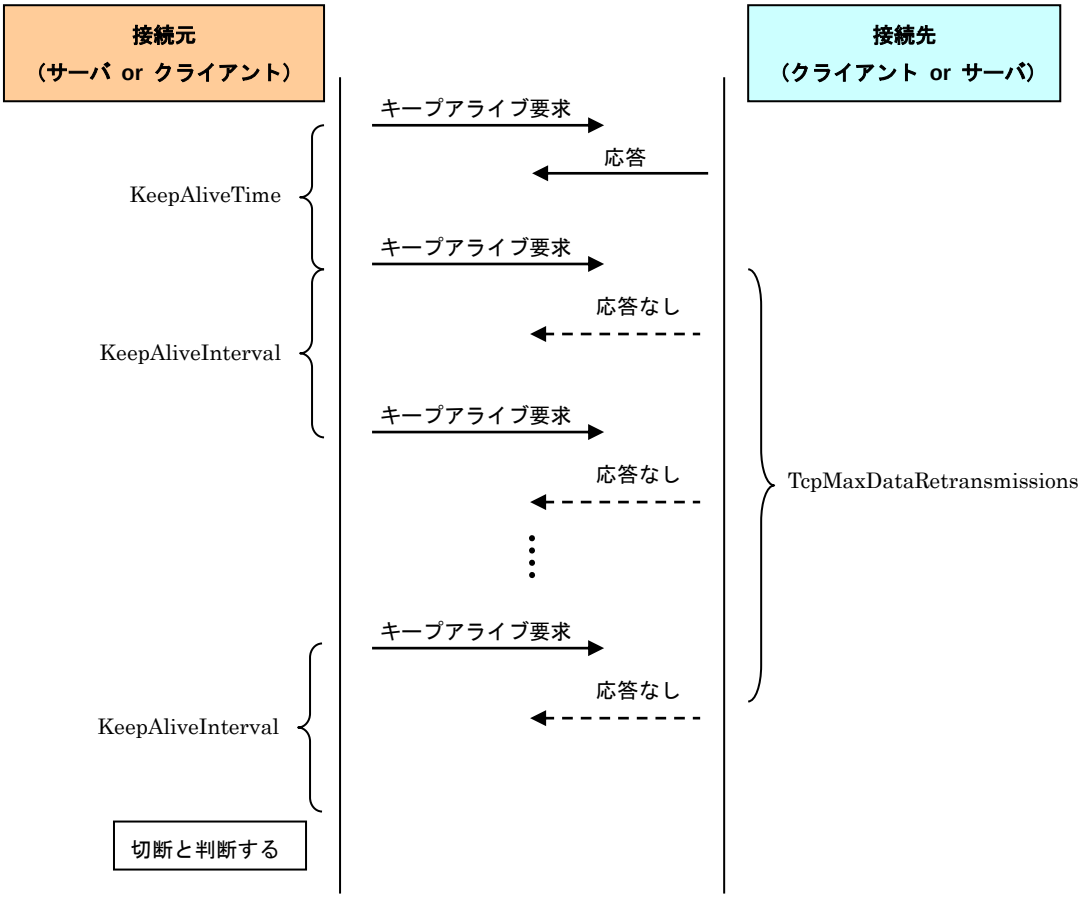


図 2.5.6　キープアライブの動作イメージ

ＴＣＰ－ＶＳＰでは、仮想 COM ポートの追加／編集ウィンドウ と オプションウィンドウによりキープアライブに関する設定値を変更できます。

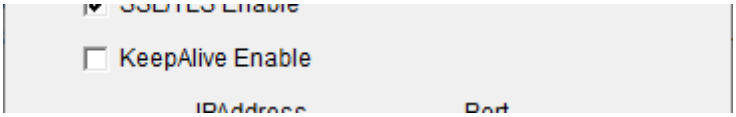


図 2.5.7　ＴＣＰ－ＶＳＰの仮想 COM ポート 追加／編集ウィンドウ（関連設定値のみ）

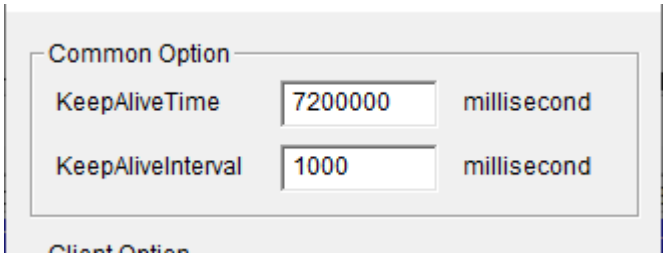


図 2.5.8　ＴＣＰ－ＶＳＰのオプションウィンドウ（関連設定値のみ）

設定項目	内容
KeepAlive Enable	キープアライブの使用／未使用の設定です。
KeepAliveTime	データ送受信が無い時に、キープアライブ要求を送信する間隔です。
KeepAliveInterval	キープアライブ要求を送信してから応答がない場合に、次のキープアライブ要求を送信するまでの時間です。

表 2.5.2　ＴＣＰ－ＶＳＰの接続の設定値

KeepAliveTime の Windows で設定されているデフォルト値は、7200000 ミリ秒となっています。
KeepAliveInterval の Windows で設定されているデフォルト値は、1000 ミリ秒となっています。
TcpMaxDataRetransmissions は、Windows で設定されているデフォルト値は、5 回となっています。（TCP-VSP では変更できません）
キープアライブパケットは、あまり頻繁に送信した場合は、障害につながる可能性がありますので、ご注意ください。

２．５．４　自動再接続

まず、ＴＣＰ－ＶＳＰでのＴＣＰ／ＩＰの接続動作について説明をします。
ＴＣＰ－ＶＳＰのＴＣＰ／ＩＰの接続動作は、一般的なＴＣＰの接続処理と同じ方法で行われます。
以下が、その動作イメージです。

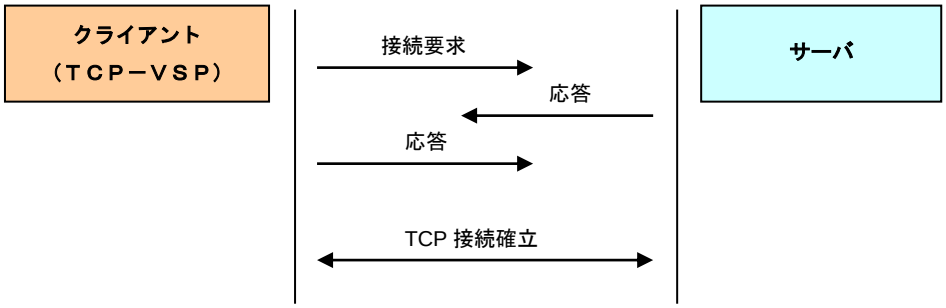


図 2.5.9　ＴＣＰ－ＶＳＰの接続動作イメージ

指定したサーバが存在しないかネットワークのトラブルにより、接続要求に対して応答が返ってこない場合は接続失敗となります。
以下が、接続を失敗した時の動作イメージです。

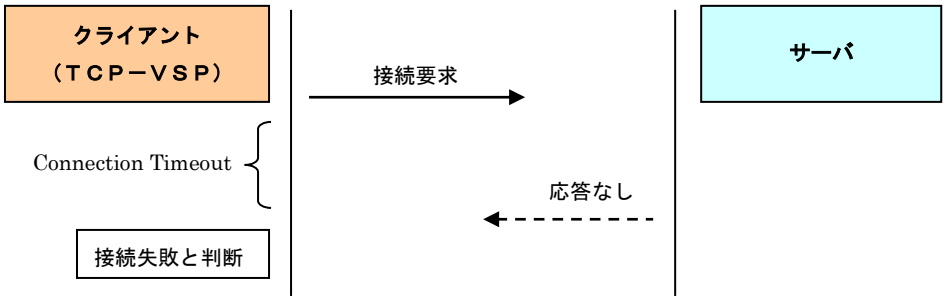


図 2.5.10　ＴＣＰ－ＶＳＰの接続失敗動作イメージ

上の図にように、接続要求に対して、指定した時間（Connection Timeout）内に接続先から応答が無かった場合は、接続失敗と判断されます。

次に、ＴＣＰ－ＶＳＰがＴＣＰ／ＩＰの切断を検出した場合の自動再接続に関して説明します。
以下が、動作のイメージ図です。

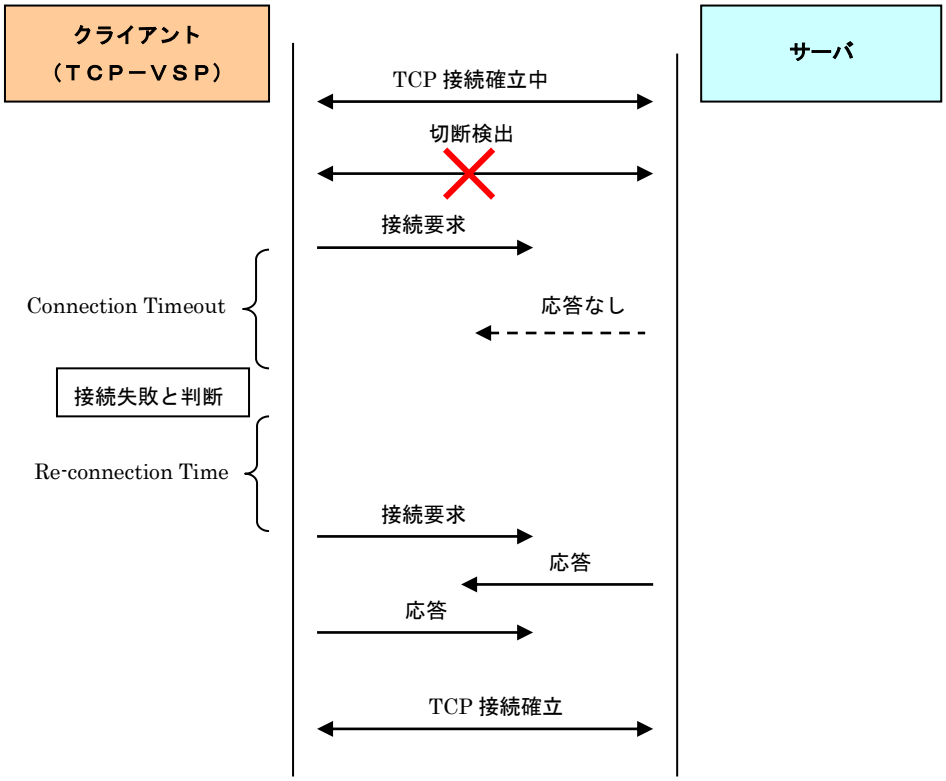


図 2.5.11　ＴＣＰ－ＶＳＰの再接続動作イメージ

ＴＣＰ－ＶＳＰが、ＴＣＰ／ＩＰの切断を検出すると、自動で接続要求を行います。
その時に、接続ができなかった場合は、指定した時間（Re-connection Time）待ち、再度接続要求を行います。

ＴＣＰ－ＶＳＰでは、オプションウィンドウにより接続（再接続）に関する設定値を変更できます。

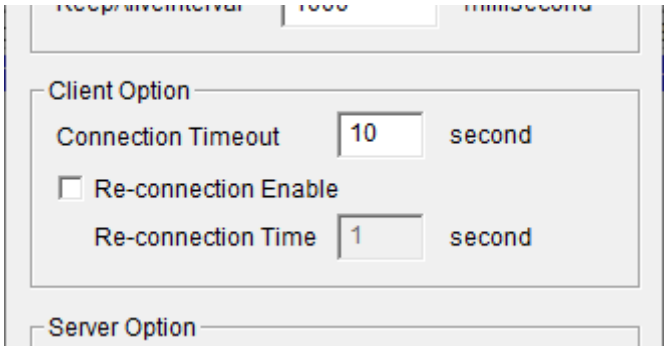


図 2.5.12　ＴＣＰ－ＶＳＰのオプションウィンドウ（関連設定値のみ）

設定項目	内容
Connection Timeout	接続失敗と判断するまでの時間
Re-connection Enable	再接続の使用／未使用
Re-connection Time	再接続までの時間

表 2.5.3　ＴＣＰ－ＶＳＰの接続の設定値

自動再接続を行わない場合は、切断を検出するとＴＣＰ－ＶＳＰに ConnectError と表示して、ＴＣＰ／ＩＰの通信は行われなくなります。

３．インストール

３．１　動作条件

TCP-VSP の動作環境

OS	Windows XP / Vista / 7 / 8 / 8.1 / 10 / 11 (Windows Vista 以降は 32bit／64bit に対応)
ハードディスク	7.8MByte 以上の空き容量
その他	Winsock Version2.0 を使用 OpenSSL 1.0.2t を使用

表 3.1.1　ＴＣＰ－ＶＳＰの動作環境

３．２　仮想ＣＯＭの仕様

作成する仮想 COM ポートの制限

ボーレート	特に制限なく使用できます
データビット長	7, 8
パリティビット	なし，偶数，奇数
ストップビット	1, 2
フロー制御	RTS/CTS, XON/XOFF

表 3.2.1　仮想 COM ポートの仕様

※ 実際の通信はネットワークの速度となりますのでボーレートは意味をもちません。表示のみの対応となります。
※ フロー制御は、仮想 COM ポートを使用するアプリケーションとＴＣＰ－ＶＳＰ間で行います。
そのため、RTS/CTS の状況 及び XON/XOFF は、ネットワーク先には伝わりません。

また、入出力制御線（DTS, DTR, DCD(CD), RI）は、以下の表の状況となります。

動作モード		DTR	DSR	DCD(CD)	RI
TCP（クライアント）	非接続	特に何も行いません	LOW レベル	LOW レベル	LOW レベル固定
	接続中		HI レベル	HI レベル	
TCP（サーバ）	非接続	特に何も行いません	LOW レベル	LOW レベル	LOW レベル固定
	接続中		HI レベル	HI レベル	
UDP		特に何も行いません	HI レベル固定	HI レベル固定	LOW レベル固定

表 3.2.2　ＴＣＰ－ＶＳＰの接続の設定値

※ 各制御線名は、仮想 COM ポートを使用する COM アプリケーション側からの名称となります。
※ BREAK 制御には、対応しておりません。
※ 各状態は、仮想 COM ポートを使用するアプリケーションとＴＣＰ－ＶＳＰ間のみとなります。
そのため、仮にネットワーク先に別の COM ポート等があったとしても、上記制御線の状況は、ネットワーク先の制御線状況とは無関係となります。

３．３　インストール

以下の手順に従ってインストールします。

１）インストール開始
“Setup.exe”を実行します。
２）インストール時の使用言語選択
English もしくは Japanese を選択します。（以降の説明では、Japanese を選択したとして説明します。）
３）TCP-VSP セットアップウィザードの開始
“次へ”ボタンを押してください。
４）インストール先の指定
インストール先をフルパスで記述します。
特に変更する必要がなければ、”次へ”ボタンを押してください。
５）プログラムグループの指定
スタートメニューに登録するショートカットのグループ名を記述します。
特に変更する必要がなければ、”次へ”ボタンを押してください。
６）インストール準備完了
設定を確認していただき、問題がなければ、”インストール”ボタンを押してください。
７）インストール状況
インストールの進行をインジケータで表示します。ここでは、何も操作しません。
８）TCP-VSP セットアップウィザードの完了
インストールの完了です。”完了”ボタンを押して終了します。

※この後に Windows を再起動する必要はありません。

３．４　起動前準備

ＴＣＰ－ＶＳＰをＳＳＬ／ＴＬＳに対応したサーバとして動作させる場合には、次の 3.4.1 節の手順に従って秘密鍵ファイルと公開鍵ファイルを作成してください。
なお、ＳＳＬ／ＴＬＳに対応したクライアント、もしくは ＳＳＬ／ＴＬＳを使用しないサーバ／クライアントとしてのみ動作させる場合には、作成作業を省略しても差し支えありません。
また、ここで説明してある内容に関しては、必要最低限の内容となりますので、詳しい内容に関しては、OpenSSL Project のホームページ（ http://www.openssl.org/ ）をご覧ください。

３．４．１　秘密鍵、公開鍵の作成

ここでの作業により秘密鍵と公開鍵ファイルを作成しますが、公開鍵ファイルは、サーバ証明書も兼ねているため２段階にわけて作成します。
まず、１段階目で、サーバ情報から証明書を作成して、２段階目に、その証明書を第３者もしくは自分自身で署名することで公開鍵ファイルを作成します。
なお、鍵ファイルを作成する時には、”openssl.exe”を使用しますが、簡単に作成できるバッチファイルを用意しました。
ここからは、バッチファイルを利用して作成する方法を説明します。

①コマンドプロンプトを起動します。

以下に、OS 毎に起動方法の参考例を記述致します。

なお、Windows Vista / 7 / 8 / 8.1 / 10 / 11 では管理者権限が必要となりますので、ご注意ください。

・Windows XP の場合

Windows のスタートメニューから「プログラム」－「アクセサリ」－「コマンドプロンプト」を選択して起動します。

・Windows Vista / 7 の場合

1）Windows のスタートメニューから「プログラム」－「アクセサリ」－「コマンドプロンプト」を右クリックします。

2）表示されたポップアップメニューから「管理者として実行」を選択します。

・Windows 8 の場合

【スタート画面から起動する場合の例】

1）スタート画面を表示する。

2）スタート画面で右クリックを行う。

3）画面下部に表示されたメニューから「すべてのアプリ」を実行する。

4）アプリ画面で、「コマンドプロンプト」を右クリックする。

5）画面下部に表示されたメニューから「管理者として実行」を実行する。

【デスクトップ画面から起動する場合の例】

1）デスクトップの左下にマウスカーソルを移動し、スタート画面アイコンを表示する。

2）スタート画面アイコンで右クリックを行う。

3）表示されたメニューから「コマンドプロンプト(管理者)」を選択する。

・Windows 8.1 の場合

【デスクトップ画面から起動する場合の例】

1）デスクトップの左下の Windows アイコンで右クリックを行う。

2）表示されたメニューから「コマンドプロンプト(管理者)」を選択する。

【スタート画面から起動する場合の例】

1）スタート画面を表示する。

2）スタート画面の下にマウスを動かし、画面下部に「↓」ボタンを表示する。

3）表示された「↓」ボタンを実行する。

4）アプリ画面で、「コマンドプロンプト」を右クリックする。

5）表示されたメニューから「管理者として実行」を選択する。

・Windows 10 / 11 の場合

【デスクトップのスタートメニューから起動する場合の例】

1）デスクトップの左下の Windows アイコンをクリックし、スタートメニューを表示する。

2）スタートメニューの「すべてのアプリ」を選択する。

3）表示されたメニューから「W」項目の「Windows システムツール」－「コマンドプロンプト」を右クリックする。

4）表示されたメニューの「その他」にマウスを移動する。

5）表示されたメニューから「管理者として実行」を選択する。

【デスクトップの右クリックメニューから起動する場合の例】

1）デスクトップの左下の Windows アイコンで右クリックを行う。

2）表示されたメニューから「Windows PowerShell (管理者)」または「コマンドプロンプト(管理者)」を選択する。（設定により PowerShell または、コマンドプロンプトが表示されます。）

②TCP-VSP のインストール先へ移動します。

```
C:¥Document and setting¥user>c:                                  入力
C:¥Document and setting¥user>cd "¥Program Files¥TCP-VSP"         入力
C:¥Program Files¥TCP-VSP>
```

なお、上記のコマンドのパスは、インストール時に c ドライブのデフォルトのインストール先を選択した場合になります。

③バッチファイルを実行します。

```
C:¥Program Files¥TCP-VSP> keycreate.bat                          入力
```

④以下のような表示が行われますので、必要事項を入力します。

```
C:¥Program Files¥TCP-VSP>openssl genrsa -des 1024 > private.key
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....................................................++++++...++++++
e is 65537 (0x10001)
Enter pass phrase:                                   入力 ①
Verifying - Enter pass phrase:                       入力 ②

C:¥Program Files¥TCP-VSP>openssl rsa -in private.key -out private.key
Enter pass phrase for private.key:                   入力 ③
writing RSA key

C:¥Program Files¥TCP-VSP>openssl req -new -days 365 -key private.key -out csr.pem -config
sample.cnf
You are about to be asked to enter information that will be incorporated into your certificate
request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [AU]:                   入力 ④
State or Province Name (full name) [Some-State]:     入力 ⑤
Locality Name (eg, city) []:                         入力 ⑥
Organization Name (eg, company) [Internet Widgits Pty Ltd]:  入力 ⑦
Organizational Unit Name (eg, section) []:           入力 ⑧
Common Name (eg, YOUR name) []:                      入力 ⑨
Email Address []:                                    入力 ⑩

C:¥Program Files¥TCP-VSP>openssl x509 -in csr.pem -out public.key -req -signkey private.key
-days 365
```

```
Loading 'screen' into random state - done
Signature ok
subject=/C=AU/ST=Some-State/O=Internet Widgits Pty Ltd
Getting Private key
```

※入力① パスフレーズとして、4～511 文字の任意の文字列を入力します。
※入力② 入力①と同じ文字列を入力します。
※入力③ 入力①と同じ文字列を入力します。
※入力④～⑩ 上記で説明したサーバ証明書のための情報を入力します。何も入力しない場合は、デフォルトとして[]で囲まれた文字列が設定されます。認証局を利用しない場合には、全て何も入力しなくても支障はありませんが、この情報がサーバ情報として接続先に送信されるため、なるべく正確に入力してください。

３．４．２　鍵作成時のコマンドの説明

> openssl genrsa -des 1024 > private.key

秘密鍵ファイル(private.key)を作成するコマンドです。
秘密鍵を作成する時に、パスフレーズの入力が求められるため、4～511 文字数の任意の文字列を入力します。

> openssl rsa -in private.key -out private.key

作成された秘密鍵からパスフレーズを削除するためのコマンドです。
実行するとパスフレーズの入力を求められますので、作成時に設定したパスフレーズを入力します。

> openssl req -new -days 365 -key private.key -out csr.pem -config sample.cnf

認証局からサイト証明書を発行してもらうためのリクエストファイル(csr.pem)を作成するコマンドです。
-days オプションによって証明書の有効期限を設定します。上記コマンドでは、365 日間有効になります。
また、-config オプションで cnf ファイルを指定します。この cnf ファイルによって、”Country Name”等の入力項目の種類を設定しますので、必要に応じて編集してから実行してください。

> openssl x509 -in csr.pem -out public.key -req -signkey private.key -days 365

認証局を使用せずに、自分で署名するためのコマンドです。

4．画面説明

4．１　メインウィンドウ

図 4.1.1　仮想ＣＯＭポート停止中の画面

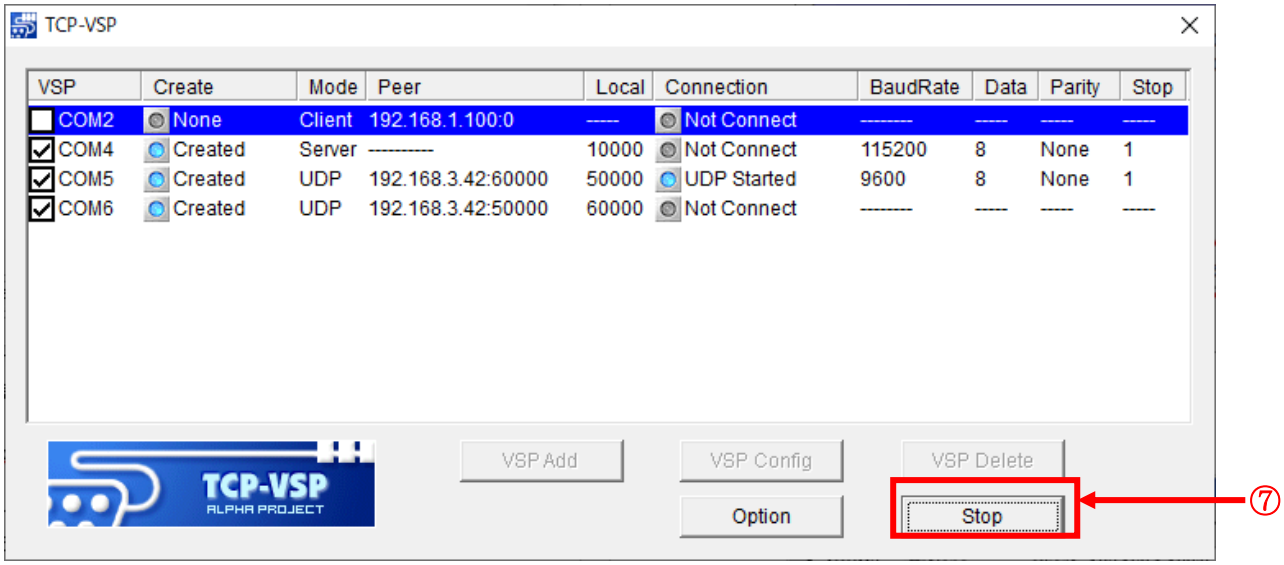


図 4.1.2　仮想ＣＯＭポート動作中の画面

①仮想 COM ポートの状態表示

各項目は、それぞれ以下のことを表示します。

VSP　：仮想 COM ポートの使用／未使用の表示 及び COM ポート番号
Create　：仮想 COM ポートの状態表示（※表 4.1.1 参照）
Mode　：動作モード（サーバ／クライアント／ＵＤＰ）の表示
Peer　：接続先の IP アドレスとポート番号の表示
Local　：受け口のポート番号の表示
Connection　：接続状態表示（※表 4.1.2 参照）
BaudRate　：ボーレートの表示
Data　：データビット長の表示
Parity　：パリティの表示
Stop　：ストップビットの表示

②"VSP Add"ボタン

仮想 COM ポートを追加するための設定ウィンドウを開きます。（※4.2 節 参照）

③"VSP Config"ボタン

仮想 COM ポートを編集するための設定ウィンドウを開きます。（※4.2 節 参照）

④"VSP Delete"ボタン

選択されている仮想 COM ポートを削除します。

⑤"Option"ボタン

全体の設定を行うウィンドウを開きます。（※4.3 節 参照）

⑥"Start"ボタン

仮想 COM ポートの処理を開始します。

⑦"Stop"ボタン

仮想 COM ポートの処理を終了します。

表示メッセージ	説明
None	仮想 COM ポート未作成
Create Error	仮想 COM ポート作成エラー
Created	仮想 COM ポート作成成功

表 4.1.1　Create 項目のメッセージ一覧

表示メッセージ	説明
Not Connection	接続していない状態
Create Error	TCP/IP(UDP)通信で使用する Socket の作成エラー
Connect Error	TCP/IP 通信の接続エラー
Connecting	接続の処理中
Connected	接続成功 及び データ通信中
SSL Error	SSL/TLS の接続エラー
SSL Connecting	SSL/TLS の接続処理中
Login Process	ユーザ認証の処理中
UDP Started	UDP 通信の準備中
UDP Error	UDP 通信エラー

表 4.1.2　Connection 項目のメッセージ一覧

４．２　仮想ＣＯＭポートの追加／編集ウィンドウ

メインウィンドウの”VSP Add”ボタン、”VSP Config”ボタンを押した時に表示されるウィンドウです。

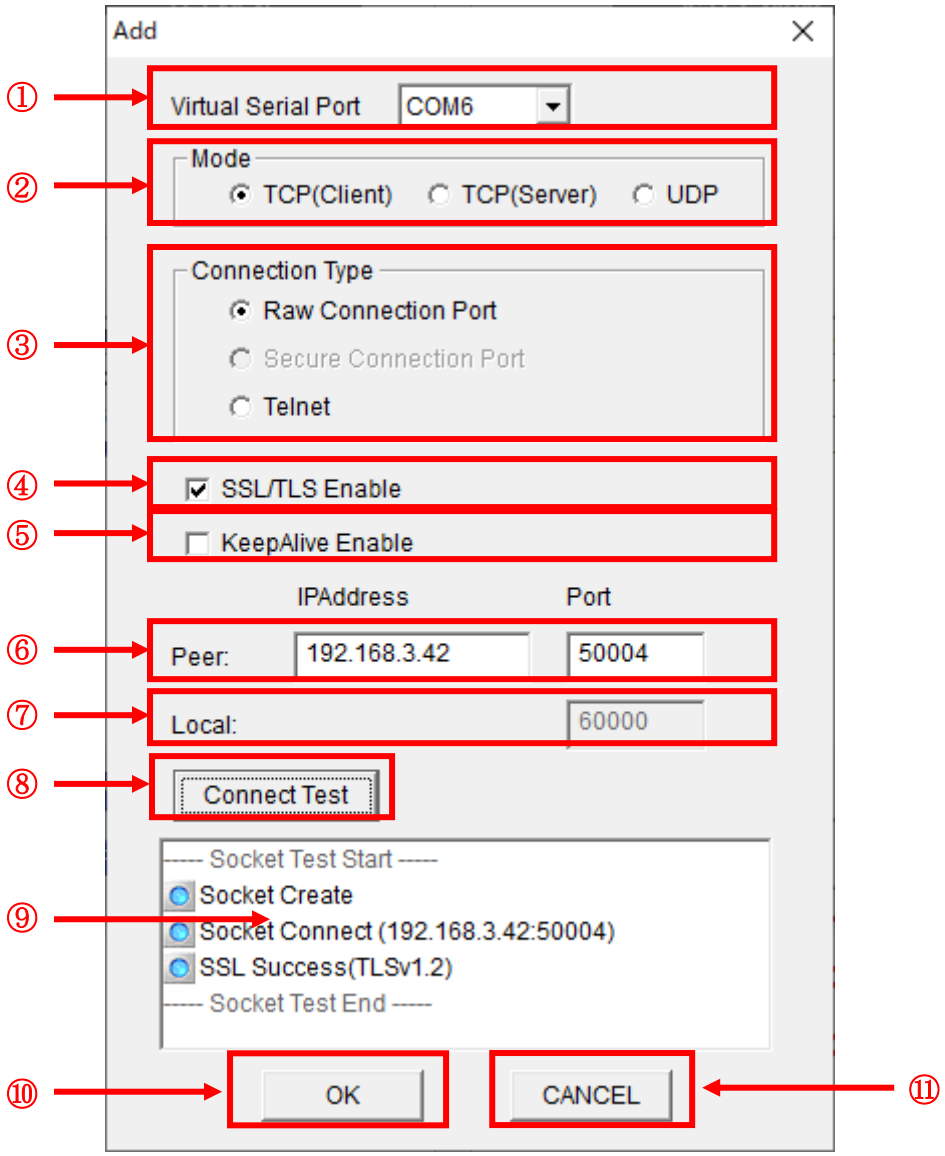


図 4. 2. 1　仮想ＣＯＭポートの追加画面

①”Virtual Serial Port”リストボックス

作成する仮想 COM ポートを選択します。

②”Mode”選択ボタン

動作モードを選択します。

③”Connection Type”選択ボタン

TCP/IP 接続時のプロトコルを設定します。各プロトコルは、以下の設定になります。

“Raw Connection Port”	：通常の接続方法になります。
“Secure Connection Port”	：接続時にユーザ名とパスワードによる認証を行います。 接続後は、”Winsock”接続と同じ動作になります。
“Telnet”	：接続中は、Telnet プロトコルに従って動作します。

④”SSL/TLS Enable”チェックボックス

SSL/TLS を使用する場合にはチェックします。

使用する SSL/TLS のバージョンは、サーバモードではクライアント側から指定されたバージョンを使用します。

クライアントモードでは、TLS1.2, TLS1.1, TLS1.0, SSL3.0 の順番でサーバ側が対応しているバージョンを使用します。

⑤”KeepAlive Enable”チェックボックス

キープアライブ要求の送信を使用する場合にはチェックします。

（キープアライブに関しては、2.5.3 切断検出 －キープアライブ－ でご確認ください。）

⑥”Peer”エディットボックス（ポート番号の設定範囲 ： 0 ～ 65535）

TCP クライアント、もしくは UDP の接続先の IP アドレス、ポート番号を設定します。

⑦”Local”エディットボックス（ポート番号の設定範囲 ： 0 ～ 65535）

TCP サーバ、もしくは UDP で使用する受け口のポート番号を設定します。

⑧”Connect Test”ボタン

設定した IP アドレス、ポート番号、SSL/TLS（使用する場合）の接続テストを行います。

接続テスト中は、接続テストをキャンセルする”Test Cancel”ボタンに変わります。

⑨結果表示領域

接続テストの結果を表示します。

⑩”OK”ボタン

仮想 COM ポートの追加／編集作業を適用してウィンドウを閉じます。

⑪”CANCEL”ボタン

仮想 COM ポートの追加／編集作業を適用しないでウィンドウを閉じます。

※1 ①の設定値は、”VSP Config”ボタンでの編集処理時には、表示のみとなります。

※2 ③は、”Mode”が”UDP”の時には、設定不可になります。
また、”Mode”が”TCP(Client)”の時には、“Secure Connection Port”のみ設定不可になります。

※3 ④、⑤は、”Mode”が”UDP”の時には、設定不可になります。

※4 ⑥は、”Mode”が”TCP(Server)”の時には、入力不可になります。

※5 ⑦は、”Mode”が”TCP(Client)”の時には、入力不可になります。

※6 ⑧は、”Mode”が”TCP(Server)”, “UDP”の時には、選択不可になります。

４．３　オプションウィンドウ

メインウィンドウの”Option”ボタンを押した時に表示されるウィンドウです。

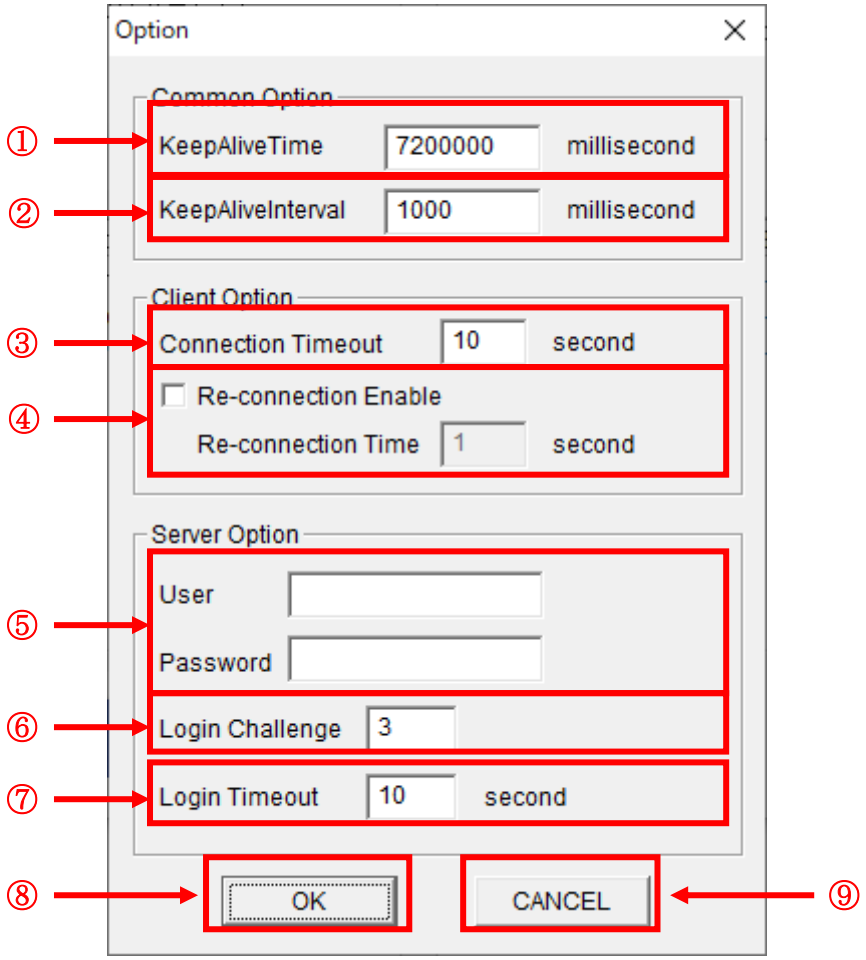


図 4.3.1　オプション設定画面

①”KeepAliveTime”エディットボックス（設定範囲　：　1　～　99999999　ミリ秒）
　キープアライブパケットの送信時間を設定します。（詳細な説明は、2.5.4 キープアライブ を参照ください。）
②”KeepAliveInterval”エディットボックス（設定範囲　：1　～　99999999　ミリ秒　）
　キープアライブパケットの送信に対する応答パケットが無かった時の次のキープアライブパケットを送信する時間を設定します。（詳細な説明は、2.5.3 切断検出 －キープアライブ－ を参照ください。）
③”Connection Timeout”エディットボックス（設定範囲　：　1　～　99　秒）
　TCP(Client)による接続時のタイムアウト時間を設定します。
④”Re-connection Enable”チェックボックス 及び 時間設定のエディットボックス（設定範囲　：　1　～　9999 秒）
　チェックを ON にすると、仮想 COM ポートが開いている限り切断を検出すると再接続を行います。
　なお、時間設定は、チェックボックスが ON の時のみ設定が可能になります。
　（詳細な説明は、2.5.4 自動再接続 を参照ください。）
⑤”User”エディットボックス 及び “Password”エディットボックス
　Login 処理のユーザ認証時に使用する User 名とパスワードを設定します。
⑥”Login Challenge”エディットボックス（設定範囲　：　1　～　9999　回）
　１度の接続で行うことができるユーザ認証回数を設定します。

⑦”Login Timeout”エディットボックス（設定範囲 ： 1 ～ 9999 秒）
Login 認証時のタイムアウト時間を設定します。タイムアウトの判断は、Login 処理中に何もデータを受信しなかった間隔が指定時間を超えた場合に起こります。
⑧”OK”ボタン
設定値を適用してウィンドウを閉じます。
⑨”CANCEL”ボタン
設定値を適用しないでウィンドウを閉じます。

※1 ①、②の設定値は、仮想 COM ポートの設定時に、”KeepAlive Enable”を設定した場合のみ有効になります。
※2 ③、④の設定値は、仮想 COM ポートの設定時に、”Mode”を”TCP(Client)”に設定した場合のみ有効になります。
※3 ⑤、⑥、⑦の設定値は、仮想 COM ポートの設定時に、”Mode”を”TCP(Server)”、”Connection Type”を“Secure Connection Port”もしくは”Telnet”に設定した場合のみ有効になります。

４．４　タスクトレイのアイコン

ＴＣＰ－ＶＳＰを起動するとタスクトレイにアイコン（図 4.4.1）が表示されます。
このアイコンを左ダブルクリックするとメインウィンドウが表示されます。
また、右クリックするとポップアップメニュー（図 4.4.2）が表示されます。各メニュー項目の動作を以下に記述します。

“ShowWindow” ：メインウィンドウを表示します。
“Exit” ：ＴＣＰ－ＶＳＰを終了します。

図 4.4.1　ＴＣＰ－ＶＳＰのアイコ

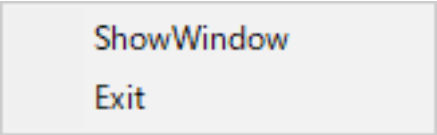


図 4.4.2　ポップアップメニュー

５．チュートリアル

５．１　アプリケーションの起動

“スタートメニュー”からインストール時に指定したプログラムグループの”TCP-VSP” - “TCP-VSP”を選択します。
デフォルトの場所は、”スタートメニュー” - “プログラム” - “AlphaProject” - “TCP-VSP” - “TCP-VSP”となります。
起動完了後に、メインウィンドウが表示されない場合には、タスクトレイに表示されたアイコンを左ダブルクリックすることで表示することができます。（4.4 節 参照）
なお、初回起動時には、以下のダイアログが表示されますので、ＣＤケースに記載されているユーザＩＤとパスワードを入力してください。

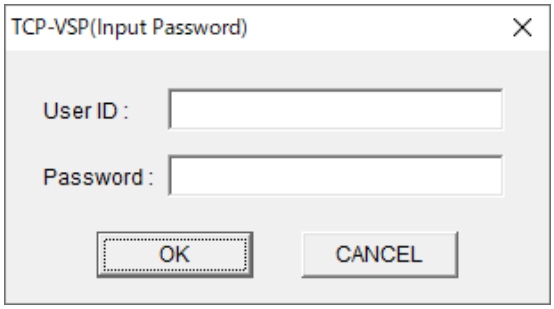


図 5.1.1　パスワード入力画面

５．２　オプションの設定

以下の手順に従ってアプリケーション全体の設定を行います。
この設定操作は、仮想 COM ポートが動作停止中の時のみ可能です。動作中の時は表示のみとなります。

１）メインウィンドウの”Option”ボタンを押します。
２）アプリケーション全体の設定を行います。
　各項目の説明は、4.3 節を参照してください。
３）“OK”ボタンを押して、オプション設定作業を完了します。

５．３　仮想ＣＯＭポートの設定

作成する仮想 COM ポートの追加、編集、削除、使用／未使用の設定を行います。
この設定操作は、仮想 COM ポートが動作停止中の時のみ可能です。

５．３．１　仮想ＣＯＭポートの追加

１）メインウィンドウの”VSP Add”ボタンを押します。
２）作成する仮想ＣＯＭポートの設定を行います。
　各項目の説明は、4.2 節を参照してください。
３）“Mode”が”TCP(Client)”の場合には、入力した”SSL/TLS”、”IPAddress”、”Port”の接続テストを行うために、”Connect Test”ボタンを押してください。この時に結果表示が、図 5.3.1 のように表示されれば成功です。
　（失敗した場合には、アイコン及び表示文字が赤くなります。また、SSL/TLS を無効にした場合には、”SSL Success”の表示はされません。）

なお、接続テスト中は、”Connect Test”ボタンが”Test Cancel”ボタンに変わり、押すことで接続テストをキャンセルすることが可能です。

4）“OK”ボタンを押して、追加作業を完了します。

５．３．２　仮想ＣＯＭポートの編集

1）登録した仮想 COM ポートの一覧の中から編集を行いたい仮想 COM ポートをマウスで左クリックします。
（選択された仮想 COM ポートの行が青で表示されます。）

2）選択した状態のまま、”VSP Config”ボタンを押します。

3）変更したい項目の編集をします。

4）“Mode”が”TCP(Client)”の場合には、仮想 COM ポートの追加の時と同様に”Connect Test”ボタンを押して、正常に接続ができることを確認します。

5）“OK”ボタンを押して編集作業を完了します。

５．３．３　仮想ＣＯＭポートの削除

1）登録した仮想 COM ポートの一覧の中から削除を行いたい仮想 COM ポートをマウスで左クリックします。
（選択された仮想 COM ポートの行が青で表示されます。）

2）選択した状態のまま、”VSP Delete”ボタンを押します。

3）仮想 COM ポートが削除されます。

５．３．４　仮想ＣＯＭポートの使用／未使用の設定

図 5.3.2 の赤い枠で囲まれている部分のチェックを ON／OFF にすることで、作成した仮想 COM ポートの使用／未使用の選択が行えます。なお、動作中での設定変更は行えません。

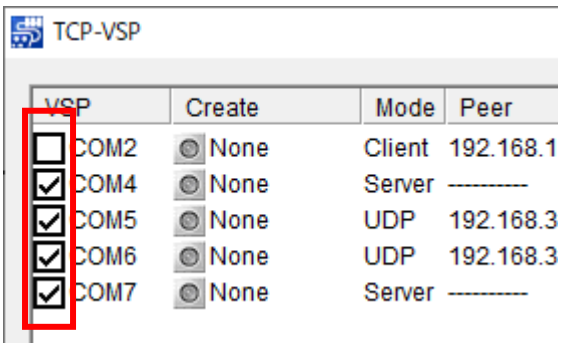


図 5.3.2　使用／未使用の選択画面

５．４　仮想ＣＯＭポートの動作開始

メインウィンドウの右下の”Start”ボタンを押して、仮想 COM ポートの動作を開始します。
使用する仮想 COM ポートが正常に作成できた場合には、メインウィンドウ上の”Create”の項目が、青いアイコンに変わり、文字列も”Created”になります。

５．５　仮想ＣＯＭポートの動作終了

仮想 COM ポートの動作を終了する時には、メインウィンドウの右下の”Stop”ボタンをします。
なお、仮想 COM ポートが開いている状態では、終了することができませんので、すべての仮想 COM ポートを閉じた状態で行ってください。

５．６　アプリケーションの終了

タスクトレイのアイコンを右クリックして表示されるポップアップメニューから、”Exit”を選択します。
この時に、終了する時の状態（仮想 COM ポート情報や開始状態 等）を保存して、次回起動時に反映します。

６．アンインストール

６．１　アンインストール

以下の手順に従ってアンインストールします。

１）TCP-VSP の終了確認
TCP-VSP が終了しているか、タスクトレイのアイコンの有無でご確認ください。
もし、アイコンが表示されている場合には、5.6 節の方法に従って TCP-VSP を終了してください。

２）アンインストール開始
“スタートメニュー”からインストール時に指定したプログラムグループにある”TCP-VSP” - “Uninstall”を選択します。
デフォルトの設定では、 ”スタートメニュー” - “プログラム” - “AlphaProject” - “TCP-VSP” - “Uninstall” となります。
Window 8.1 の場合は、”コントロールパネル” - “プログラムのアンインストール” を表示し、”TCP-VSP” をアンインストールしてください。
Window 10 / 11 の場合は、”設定” - “アプリ” を表示し、”TCP-VSP” をアンインストールしてください。

３）アンインストール確認
“TCP-VSP”とその関連コンポートネントをすべて削除します。よろしいですか？”の質問に、”はい”を選択します。

４）アンインストール状況
アンインストールの進行をインジケータで表示します。ここでは、何も操作しません。

５）アンインストール完了
正常にアンインストールが完了しますと、”ご使用のコンピュータから正常に削除されました。” のメッセージが表示されます。
“OK”ボタンを押して終了します。

※この後に Windows を再起動する必要はありません。

７．その他

７．１　ＦＡＱ

Ｑ１．　相手先が異常切断しても”Ｃｏｎｎｅｃｔｉｏｎ”項目の表示が”Ｃｏｎｎｅｃｔｅｄ”と表示されたままになる。

Ａ１．　相手先の電源が落ちる等の原因により、ＴＣＰ／ＩＰポートが異常切断した場合、次のデータ送信時からの送信タイムアウト（最大約３分間）後に”Ｃｏｎｎｅｃｔ　Ｅｒｒｏｒ”と表示されます。
その間の表示は”Ｃｏｎｎｅｃｔｅｄ”と表示してしまいますので、ご注意ください。
→ ＴＣＰ－ＶＳＰ　Ｖｅｒ１．２０以降では、キープアライブの機能を追加しました。詳しくは、「2.5 接続維持機能」でご確認ください。

Ｑ２．　データ通信中に自動再接続されたが、相手先で受信できなかったデータがある。

Ａ２．　異常切断から送信タイムアウトまでに送信されたデータに関しては、その後再接続したとしても再送信が行われません。ご了承ください。

Ｑ３．　ＴＣＰ／ＩＰポート側が切断されていても仮想ＣＯＭポート側のＤＳＲ信号がＨｉの状態になる。

Ａ３．　ＤＳＲ信号に関しては、ＴＣＰ／ＩＰの接続先のトラブル等でデータ通信が正常にできなくなってもＨｉの状態のままになる時があります。ＤＳＲ信号は、ＴＣＰ－ＶＳＰがＴＣＰ／ＩＰの状態を切断と判断した場合にＬｏｗとなりますので、ご注意ください。
ＴＣＰ／ＩＰの切断の判定は、「2.5 接続維持機能」も合わせてご確認ください。

Ｑ４．　その他の仮想ＣＯＭポートを作成するアプリケーションと併用が可能か？

Ａ４．　ＴＣＰ－ＶＳＰ以外の仮想ＣＯＭポートを作成するアプリケーションと併用で使用した場合、不具合が起こる可能性があります。
ＴＣＰ－ＶＳＰをインストールする前に、その他の仮想ＣＯＭポートを作成するアプリケーションをアンインストールしてからご使用ください。

Ｑ５．　フロー制御のＸＯＮ／ＸＯＦＦを使用する場合の注意することは？

Ａ５．　ＴＣＰ－ＶＳＰ　Ｖｅｒ１．２０以降では改善していますが、以前のバージョンでは、以下の不具合が発生します。
作成した仮想ＣＯＭポートをソフトウェアフロー制御（ＸＯＮ／ＸＯＦＦ）により開いた時、仮想ＣＯＭポート側からＥｔｈｅｒ側に大量のデータが送信された場合に、不具合が発生します。
詳しい症状及び対策に関しては、アプリケーションノート(ＡＮ４０４)をご覧ください。

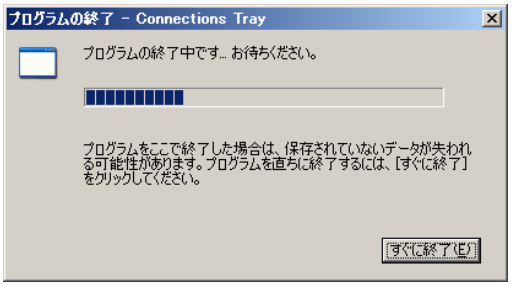
Ｑ６．　仮想ＣＯＭポートを比較的多く利用する場合に、仮想ＣＯＭポートを削除してすぐに仮想ＣＯＭポート作成時にＴＣＰ－ＶＳＰが応答なしとなる場合がある。

Ａ６．　仮想ＣＯＭポート削除した場合に、ＴＣＰ－ＶＳＰでは終了していてもＷｉｎｄｏｗｓ側で終了処理を行っています。その時に、仮想ＣＯＭポートを作成した場合に、作成に時間がかかり応答なしになる場合があります。
この時には、ＴＣＰ－ＶＳＰの右上の×ボタンを押さずにしばらくお待ちください。

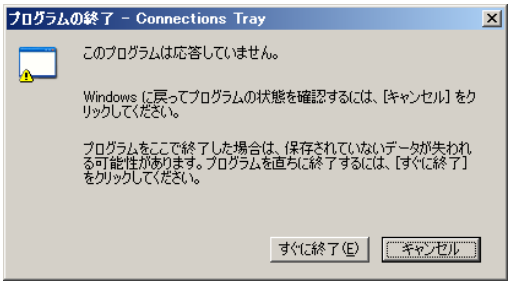
Ｑ７．　仮想ＣＯＭポートを比較的多く利用する場合に、仮想ＣＯＭポートを削除してすぐに仮想ＣＯＭポート作成を行うと、ＣＯＭポート作成時に”Ｃｒｅａｔｅ　Ｅｒｒｏｒ”となる場合がある。

Ａ７．　理由はＡ６と同様になります。
起こる場合は、仮想ＣＯＭポートを削除してから次の作成開始まで少し待つようにしてください。

Ｑ８．　仮想ＣＯＭポートを比較的多く利用する場合に、仮想ＣＯＭポートを作成したまま、Ｗｉｎｄｏｗｓを終了（再起動）する場合に、以下のようなプログラム終了メッセージが表示される場合がある。



Ａ８．　理由はＡ６、Ａ７と同様になります。
このようになる場合は、すぐに終了ボタンを押さずにしばらくお待ちください。
また、しばらく待っても終了できない場合は、以下のメッセージが表示されます。その場合、キャンセルボタンを押してから、もう一度Ｗｉｎｄｏｗｓの終了（再起動）を行ってください。



７．２　ネットワーク用語解説

ＴＣＰ (Transmission control protocol)	２種類あるＩＰの上位プロトコルのひとつ。もうひとつのＵＤＰに比べ、コネクション型でパケット毎の応答確認機能等があり信頼性が高い。ＲＦＣ７９３で規定。
ＩＰ (Internet protocol)	米国防総省のネットワークプロジェクトで開発されたプロトコルで、インターネットに接続される機器は、全てこの共通プロトコルを使用している。上位層にはＴＣＰやＵＤＰ等がある。
ＴＣＰ／ＩＰ	ネットワーク層にＩＰ、上位にＴＣＰを使うプロトコルの名称。インターネットの標準プロトコルである。上位のアプリケーション層のプロトコルとしては、ＨＴＴＰ、ＦＴＰ、ＴＥＬＮＥＴ、ＳＭＴＰ、ＤＮＳ、ＳＮＭＰ等がある。
ＵＤＰ (User datagram protocol)	ＩＰの上位プロトコルのひとつ。ＲＦＣ７６８で規定。ＴＣＰに比べ処理の負荷が軽いため、高速処理が可能だが、コネクションレス型で信頼性に劣る。
ＩＣＭＰ	ＩＰプロトコルの状態に関する情報を管理するプロトコル。ＰＩＮＧ等の応答に使われる。

ＰＩＮＧ	ＴＣＰ／ＩＰネットワーク上の任意のコンピュータに対して接続を確認するためのコマンド。
ＡＲＰ (Address resolution protocol)	アドレス解決プロトコル。ＩＰアドレスから、ＭＡＣアドレスを取得するためのプロトコル。逆にＭＡＣアドレスからＩＰアドレスを取得するプロトコルはＲＡＲＰと呼ばれる。
ＴＥＬＮＥＴ	ネットワーク上の他のコンピュータに接続して遠隔操作を実現するためのプロトコル。
ＦＴＰ (File transfer protocol)	インターネット上の２点間でファイル転送を行うためのプロトコル。ＲＦＣ９５９で規定。
ＬＡＮ (Local Area Network)	会社内などのある限定された範囲内のネットワーク。最近ではイーサネットなどの技術そのものをＬＡＮと呼ぶ場合がある。
ＷＡＮ (Wide Area Network)	限定されたエリアを超えて接続される広域ネットワーク。ＬＡＮの対比語としても用いられる。
ＰＰＰ (Point To Point Protocol)	２点間の通信に使用するプロトコル。インターネットプロバイダとダイアルアップ接続する場合等に用いられる。ＲＦＣ１６６１で規定。
ＰＰＰｏＥ (PPP Over Ethernet)	ＰＰＰのリンク手順をイーサネット上で実行する仕様。ＡＤＳＬ（フレッツＡＤＳＬ、イーアクセス）で採用されている。ＲＦＣ２５１６で規定。
ＰＰＰｏＡ (PPP Over ATM)	ＡＴＭネットワーク上からＰＰＰのやり取りを規定した技術。ＡＤＳＬ（ＯＣＮ、ＡＣＣＡ）で採用されている。ＲＦＣ２３６４で規定。
ＡＤＳＬ	既存の電話線ケーブルを使用する高速デジタル伝送方式。ｘＤＳＬの中でも最も代表的な伝送技術。ＮＴＴのフレッツＡＤＳＬ等が採用している。
ＡＴコマンド	モデム等を制御するためのコマンド体系の総称。コマンドの先頭は必ず'ＡＴ'から始まる。
ポート番号	ＴＣＰまたはＵＤＰが備える機能で、同一パソコン上で複数のネットワークアプリケーションを実行させるための仕組み。ネットワークから受け取ったパケットをどのアプリケーションに引き渡すかポート番号で特定することができる。 ポート番号は０～６５５３５までであるが、０～１０２３までは Well Known Port、１０２４～４９１５１までが Registered ポートとなっており、使用方法が規定されている。４９１５２～６５５３５は、Dynamic/Private ポートとなっており、自由に使用することができる。
ＷｅｌｌＫｎｏｗｎポート	ＩＣＡＮＮが規定している予約されたポート番号。FTP→20/21,TELNET→23、SMTP→25、DNS→53、HTTP→80、POP3→110、SMTP→161 などと決められている
ＤＨＣＰ	クライアントに動的にＩＰアドレスを割り当て、切断時に回収するためのプロトコル。

ＭＡＣアドレス	ネットワーク機器一つ一つに割り当てられる番号。全４８ビットで、先頭２ビットが、ユニキャストかマルチキャストかを示すＩ／Ｇビット、続く２２ビットが各製造メーカに割り当てられた番号、残り２４ビットが各メーカが機器にユニークに割り当てる番号となっている。したがって、各機器のＭＡＣアドレスは世界で一つしかない。
ＩＰアドレス	ＩＰプロトコルで使用される各コンピュータに割り当てられるアドレス。全３２ビットとなっている。通常は８ビット単位で区切られ、１０進数で表される。(例 192.168.1.1)
サブネットマスク	ＩＰアドレスの、どこまでがネットワーク番号として割り当てられたビットなのか識別、通知するための値。ＩＰアドレスと同じで全３２ビットで、８ビット単位で区切られ、１０進数で表される。(例 255.255.255.0)
ＧＡＴＥＷＡＹ	ネットワーク上で、媒体やプロトコルが異なるデータを相互に変換して通信を可能にする機器。
グローバルＩＰ（アドレス）	インターネットに接続された機器に一意に割り当てられた IP アドレス。インターネットの中での住所にあたり、インターネット上で通信を行うためには必ず必要である。IANA が一元的に管理しており、各国の NIC によって各組織に割り当てられる。
ローカルＩＰ（アドレス）	組織内のネットワークに接続された機器に一意に割り当てられた IP アドレス。NIC に申請を行わなくても組織内で自由に割り当てることができるが、インターネット上での一意性は保証されないため、そのままではインターネットを通じて通信を行うことはできない。プライベートアドレスしか持たない機器がインターネットで通信を行うには、グローバルアドレスを割り当てられた機器に NAT や IP マスカレード、プロキシなどの手段によって中継してもらう必要がある。
スタティック（静的）アドレス	ネットワーク上の各クライアントに固定 IP アドレスを割り当てる方式。静的 IP アドレス指定を使用しているネットワークでは、ネットワーク管理者が各コンピュータに IP アドレスを手動で割り当てる。静的 IP アドレスを割り当てられると、IP アドレスが手動で変更されない限り、コンピュータは起動するごとに同じ IP アドレスを使用してネットワークにログオンする。
ダイナミック（動的）アドレス	スタティックアドレスとは反対に、接続するたびにＩＰアドレスを割り当てられる方式。ＩＰアドレスの割り当てはＤＨＣＰサーバにて行われる。ダイアルアップ接続はこの方法が用いられる。
ピア・ツー・ピア	コンピュータ同士を１対１で接続する通信方式。
サーバ	コンピュータネットワークにおいて、クライアントコンピュータに対し、自身の持っている機能やデータを提供するコンピュータのこと。サーバはクライアントからの接続要求により接続される。
クライアント	コンピュータネットワークにおいて、サーバコンピュータの提供する機能やデータを利用するコンピュータのこと。クライントはサーバへ接続要求を出すことによりサーバと接続される。

パケット	コンピュータ通信において、送信先のアドレスなどの制御情報を付加されたデータの小さなまとまりのこと。データをパケットに分割して送受信する通信方式をパケット通信と呼ぶ。
フローコントロール	ＲＳ２３２Ｃ通信等で、データのオーバーフローを防ぐために、送受信を制御するための仕組み。ＲＴＳやＣＴＳ等の制御線を用いる場合は、ハードウェアフローコントロールと呼ばれる。
トラフィック	ネットワーク上を一定時間内に流れる情報量のこと。トラフィックの多さに比例して、情報伝達遅延や損失等の比率が高くなる。
ＲＦＣ	インターネットに関する技術の標準を定める団体である IETF が正式に発行する文書。IP(RFC 791)、TCP(RFC 793)、HTTP(RFC 2616)、FTP(RFC 959 など)などインターネットで利用されるプロトコルや、その他インターネットに関わるさまざまな技術の仕様・要件を、通し番号をつけて公開している。
ＩＳＰ (Internet Service Provider)	インターネットアクセスプロバイダのこと。
ＳＳＬ (Secure Socket Layer)	トランスポート層でＴＣＰ／ＩＰ通信のセキュリティを確保するためのプロトコル。Netscape Communication 社が提案した。
ＴＬＳ (Transport Layer Security)	Netscape Communication 社が提案したＳＳＬ３．０のＩＥＴＦによる標準化版。バージョン１．０はＲＦＣ２２４６で規定されている。

製品サポートのご案内

●バージョンアップ

本製品は、不定期で更新されます。
更新内容は、弊社ホームページにて確認できます。

●弊社ホームページのご利用について

お客様にお役立ていただける情報を弊社ページに掲載しておりますので、是非ご利用ください。

TCP-VSP	https://www.apnet.co.jp/product/eztcp/tcp-vsp.html
TCP-VSP for ezTCP	https://www.apnet.co.jp/product/eztcp/tcp-vsp_for_ez.html

●ユーザ登録について

ユーザ登録は、弊社ホームページ、または FAX にて受け付けております。
ユーザ登録をしていただきますと、製品サポートのほか、ご希望のお客様には、新製品やバージョンアップをメールにてご案内させていただきます。

●製品サポートの方法

製品サポートを受ける為には事前にユーザ登録が必要です。
製品サポートについては、FAX もしくは E-Mail でのみ受け付けております。お電話でのお問い合わせは受け付けておりませんので、ご了承ください。なお、お問い合わせの際には、製品名、シリアルナンバー（ユーザ ID)、使用環境、使用方法、問題点などを詳細に記載してください。

製品に関するお問い合わせ

ユーザーサポート	https://www.apnet.co.jp/support/query.html

●製品サポートについて

本製品を利用したアプリケーションプログラムの作成方法とそれらに関連するご質問は、受け付けておりません。
本製品のソフトウェア技術に関するご質問は、一切受け付けておりません。
本製品を利用したネットワークの構築のご提案や外部機器との接続可否の確認については有償にて承ります。
海外での保守サービス及び技術サポート等はおこなっておりません。

エンジニアリングサービスのご案内

弊社製品をベースとしたカスタム品やシステム開発を承っております。
お客様の仕様に合わせて、設計から OEM 供給まで一貫したサービスを提供いたします。
詳しくは、弊社営業窓口までお問い合わせください。

エンジニアリングサービスに関するお問い合わせ

受託開発	https://www.apnet.co.jp/engineering/index.html
E-Mail	sales@apnet.co.jp

改定履歴

版数	日付	改定内容
1 版	2004/08/02	新規
2 版	2004/09/28	UDP に関する記述を追加，初回起動時のパスワード入力画面の説明を追加 画面説明の SSL/TLS チェックボックスの説明を修正
3 版	2005/01/14	対応 OS の注意書き削除 オプションウィンドウの項目追加
4 版	2007/11/22	「３．１ 動作条件」のフロー制御から XON/XOFF を削除 「７．１ ＦＡＱ」にＱ５～Ｑ８を追加
5 版	2008/06/23	全体的に文章を変更。主には、以下の節を変更。 「２．５ 接続保持機能」の追加 「３．１ 動作条件」の変更 「３．２ 仮想 COM の仕様」の追加 「３．４．１ 秘密鍵、公開鍵の作成」の手順変更 「４．２ 仮想ＣＯＭポートの追加／編集ウィンドウ」の変更 「４．３ オプションウィンドウ」の変更 「７．１ ＦＡＱ」のＡ１、Ａ３、Ａ５を変更
5.1 版	2010/12/20	梱包内容変更 対応 OS 変更
5.2 版	2015/12/16	対応 OS 及び ハードディスクの使用容量の変更 「３．４．１ 秘密鍵、公開鍵の作成」のコマンドプロンプト起動方法の追加
5.3 版	2020/03/13	TCP-VSP の動作環境の変更 SSL2.0 削除 TLS1.2/1.1 追加 製品サポートの内容を更新
5.4 版	2023/10/02	対応 OS を更新 住所を更新

著作権及びサポートについて

・本製品「TCP-VSP」（以下、本ソフトウェア）の著作権はアルファプロジェクトが保有します。
　本ソフトウェアを無断で譲渡、転売、２次配布することは一切禁止いたします。
・当社は本ソフトウェアに関し、海外での保守サービス及び技術サポート等は行っておりません。
・本ソフトウェアの運用の結果、万一損害が発生しても、弊社では一切責任を負いませんのでご了承ください。

本文書について

・本文書の著作権は、株式会社アルファプロジェクトが保有します。
・本文書の内容を無断で転載することは一切禁止します。
・本文書の内容は、将来予告なしに変更されることがあります。
・本文書の内容については、万全を期して作成いたしましたが、万一ご不審な点、誤りなどお気付きの点がありましたら弊社までご連絡下さい。
・本文書の内容に基づき、アプリケーションを運用した結果、万一損害が発生しても、弊社では一切責任を負いませんのでご了承下さい。

商標について

・Windows®の正式名称は Microsoft®Windows®Operating System です。
　Microsoft、Windows、Windows Vista は、米国 Microsoft Corporation.の米国およびその他の国における商標または登録商標です。
　Windows®11、Windows®10、Windows®8.1、Windows®8、Windows®7、Windows Vista®、Windows®XP は、米国 Microsoft Corporation.の商品名称です。
　本文書では下記のように省略して記載している場合がございます。ご了承ください。
　Windows®11 は Windows 11 もしくは Win11
　Windows®10 は Windows 10 もしくは Win10
　Windows®8.1 は Windows 8.1 もしくは Win8.1
　Windows®8 は Windows 8 もしくは Win8
　Windows®7 は Windows 7 もしくは Win7
　Windows Vista®は Windows Vista
　Windows®XP は Windows XP もしくは WinXP
・会社名、製品名は、各社の登録商標または商標です。

ALPHAPROJECT
株式会社アルファプロジェクト
〒431-3114
静岡県浜松市中央区積志町 834
https://www.apnet.co.jp
E-Mail: query@apnet.co.jp