

HPE

GreenLake

無計画なハイブリッドクラウドから
計画的なハイブリッドクラウドへ。
かしこい選択。

概要解説をダウンロード

@IT > クラウド > Windows Server Insider > 第15回 信頼性のある通信を実現するTCPプロトコル...

基礎から学ぶWindowsネットワーク

第15回 信頼性のある通信を実現するTCPプロトコル（2）

（3/3 ページ）

2004年01月29日 00時00分 公開

[デジタルアドバンテージ, 著]

印刷

通知

見る

Share

10

前のページへ

1

2

3

さてそれでは、実際のTCP接続の詳細について見てみよう。TCP接続の概要についてはすでに前回述べているので繰り返さないが、簡単に復習しておく、「データを送信したら、それに対する応答（ACK）を必ず確認する」ということである。一見複雑そうに見えるTCP通信の内容も、この原則さえ分かっていたら容易に理解できる。そしてこの原則は、コネクションのオープンやクローズ時にも徹底されているのが分かるだろう。

TCP接続のオープン

UDPによる通信と違って、TCPでは実際の通信に先立って、いろいろな準備が必要である。この準備のことをオープンといい、逆に通信が終了するための処理のことをクローズという。

TCPによる通信ではシーケンス番号に基づいた送受信確認が大事な役割を担っているが、オープン処理は、このシーケンス番号の初期値をお互いに交換（通知）するところから始まる。そして双方の持つシーケンス番号が正しく相手に伝わったことが確認できて、オープン処理が完了する。具体的には、自分の持つシーケンス番号を相手に通知してTCP接続をオープンする意思を相手に伝え、それに対する受信確認を待つ。通信相手の方でも同様に、シーケンス番号を相手に通して、それに対する受信確認を待つ。双方で同様のことを実行するのは、TCPが双方向通信を実現しているからである。送信もしくは受信だけしかない場合でも、この手続きは省略することはできず、双方がシーケンス番号の通知と受信確認を行わなければならない。

実際のオープン時のTCPパケットのやりとりを詳しく見ると、次のようになっている。全部で3つのパケットが行き来しているので、これを「3ウェイ・ハンドシェイク」という。

検索

ホワイトペーパー

- 

障害対応を迅速化、ネットワーク監視ツールの選定で押さえるべき3つのポイント
- 

検知してからどうするか!? 標的型サイバー攻撃における内部対策の提案
- 

ネットワーク製品の導入に関する読者調査レポート(2014年12月)
- 

もう「Wi-Fi 7」時代? 無線LANの気になる進化

HPE

GreenLake


無計画なハイブリッドクラウドから
計画的なハイブリッドクラウドへ。
かしこい選択。


スポンサーからのお知らせ - PR -

「ネットワークが分からない」状態からでも丸ごとサポート

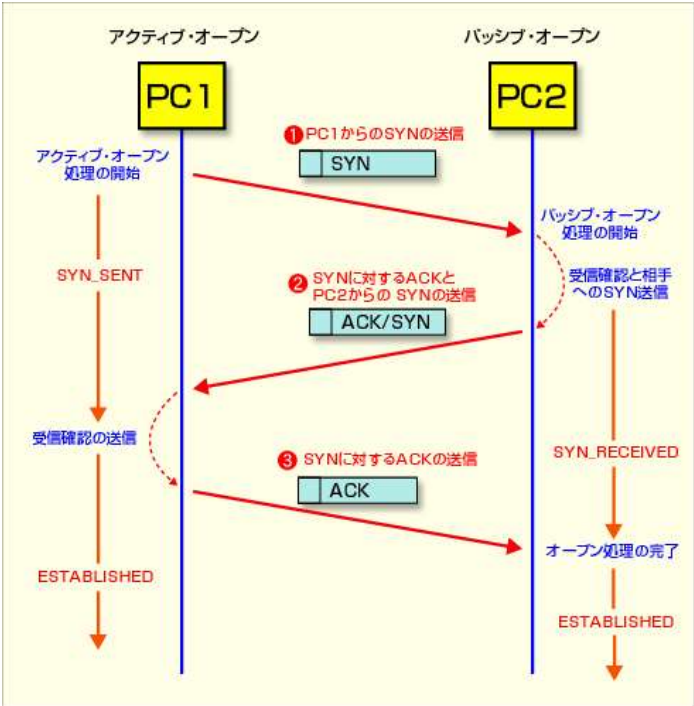
重要なのは発展性 なぜ今、“ストレージ”に注目が集まっているのか

Special - PR -

- 

複数ベンダーの「継ぎはぎSASE」で生じる課題、どうすれば解決できるのか？
- 

「ほとんど誰も見ていない」社内ポータル、どう変えるべき？
New!
- オンプレのハードウェアも「サブスク」の時代へ
コストや契約はどう変わる？



3ウェイ・ハンドシェイクによるTCP接続のオープン処理
オープン処理は、双方からSYN/パケットを送信し、それぞれに対してACK/パケットで確認応答を返している。SYNとACKを同じパケットに載せることにより、3パケット（3ウェイ・ハンドシェイク）でオープン処理が完了する。先にオープン要求（SYN/パケット）を送信する方をアクティブ・オープン、そうでない方をパッシブ・オープンという。SYNは Synchronizeの略であり、シーケンス番号とACK番号を同期させるために使われる。「SYN_SENT」や「ESTABLISHED」「SYN_RECEIVED」はTCPの内部的な状態を表す文字列（詳細は次回解説）。

TCPはポイント・トゥ・ポイントのストリーム型通信を実現するサービスであり、双方向で完全に対称な通信を行う。だがオープン時には2台のコンピュータで少し役割が異なる。つまりオープン要求を先に相手に送信する方（図中のPC1）と、そのオープン要求を受ける方（PC2）の2種類の役割が存在する。

左側のPC1のように、自分の方から相手に対して先にオープン要求を送信することを「アクティブ・オープン」といい、右側のPC2のように、相手からのオープン要求を待ち受けしてオープンすることを「パッシブ・オープン」という。またオープン要求を待っている状態を「リッスン（listen）」状態という。一般的には、まずサーバ側（サービスを提供する側）がリッスン状態に入ってクライアントからのオープン要求を待ち、そこにクライアント側から接続要求を送信することによって、TCP接続を確立する。



Special
オンプレのハードウェアも「サブスク」の時代へ コストや契約はどう変わる？

このオープン処理の手順を詳しくみると、次のようになる。

■手順1（1）—PC1からのオープン要求の送信

オープン処理は、まずSYNフラグをセットしたTCPパケットを相手に送信するところから始まる。シーケンス番号フィールドには適当な32bitの数値をセットしておく（数値自体には意味はなく、任意でよい）。ACKフィールドは未定なので0で埋めておく。オプション・フィールドには、一般的にはMSS（Maximum Segment Size）をセットしておく（MSSについては次回解説）。またウィンドウ・サイズ・フィールドにはPC1側の受信バッファのサイズを反映した値をセットしておく。そのほかのフィールドも適宜セットし、PC2に向けて送信する。



自分が作ったアプリがスマホで動くさまを見ると、学生の目が輝きます New!



社内ルールだけでは限界 有名無実化した「ローカル保存禁止」にどう対応？



「ネットワークが分からない」状態からでも丸ごとサポート New!



「守る」だけでは不十分 今どきのストレージには何が必要？



データは「守りながら活用する時代」に

@IT Special

Windows Server Insider 記事ランキング

本日	月間
Excel（エクセル）で日付から自動的に曜日を入力する	
【Excel】重複データを色付けして瞬時にダブリをチェックする	
【Excel】パスワードロックを強制的に解除する方法	
TCP/IP通信の状態を調べる「netstat」コマンドを使いこなす【Windows OS】	
Windows OSのdirコマンドでファイル名の一覧を取得する	
システム要件を満たさないPCをWindows 11 2023 Update（23H2）にアップデートする方法	
【Windows 10／11】えっ、UTF-8じゃなくてShift-JISで？ お手軽文字コード変換方法まとめ	
PDFファイルにキーボードから直接文字入力する方法【本家Acrobat Reader編】	
Excelの落とし穴「先頭のゼロ（0）」問題の対処法	
【Windows 10／11】PCが数分で勝手にスリープするのを防ぐ	

ランキングをもっと見る

あなたにおすすめの記事

- PR -



自分が作ったアプリがスマホで動くさまを見ると、学生の目が輝きます New!



社内ルールだけでは限界 有名無実化した「ローカル保存禁止」にどう対応？

■手順2 (2) - オープン要求に対する応答と、PC2からのオープン要求の送信

(1) に対する応答として、ACKフラグをセットし、ACK番号フィールドには、受信したパケットのシーケンス番号フィールドの値に1を加えたものをセットする。またPC2からのオープン要求を表すために、SYNフラグをセットし、シーケンス番号フィールドには適当な32bitの数値をセットしておく（この値はPC1のシーケンス番号とは関係がなく、まったく別の32bitのランダムな数値を使えばよい）。さらにオプションやウィンドウ・サイズ・フィールドなども適宜セットし、PC1に向けて送信する。オプションやシーケンス番号フィールドの値は、PC1のものとはまったく関係なく、独自に設定すればよい。

■手順3 (3) - PC2からのオープン要求に対する応答

PC1では、ACKとSYNがセットされたパケットを受け取ることで、最初送信したオープン要求が正しく受け付けられたことを確認する。またPC2からのSYNに対しては、ACKフラグをセットしたパケットを使って応答し（ACK番号フィールドは、「受信したシーケンス番号+1」とする）、オープン要求を受け付けたことをPC2に通知する。この時点でPC1のオープン処理が完了する。また送信されたACKパケットがPC2に届いた時点で、PC2もオープン処理を完了する

以上の3つの手順により、TCP接続のオープン処理は完了する。

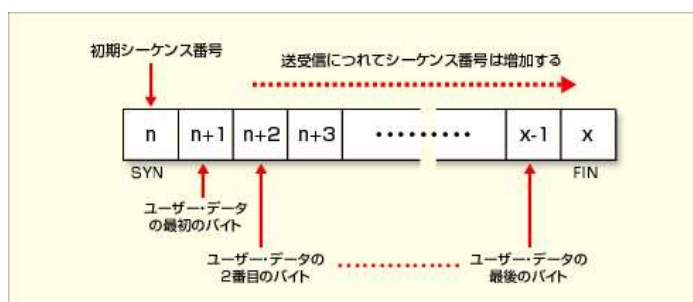
シーケンス番号について

ここでシーケンス番号について少し補足しておこう。

シーケンス番号は、データの送信元が提供する、32bitの数値である。データを受信した側では、このシーケンス番号に基づいて、どの部分までのデータを受信したかを応答している。

シーケンス番号の初期値は、オープン手順の解説で述べたように、各TCP接続ごとにランダムに決められ、相手側へと通知される。そしてデータを受信するたびに、受信したデータのbytes数に応じてACK番号を更新し、送信元へ受信確認を返信する。

ところでこのシーケンス番号は、ユーザー・データ1byteにつき、1つずつ増加するのが基本であるが、2つだけ例外がある。次の図のように、オープン時のSYNフラグと、クローズ時のFINフラグにもシーケンス番号がそれぞれ1つずつ割り当てられているのである（クローズ処理については後述）。



シーケンス番号

シーケンス番号はユーザーのデータだけでなく、仮想的に、SYNとFINのフラグにも割り当てられている。4Gbytesを超えるとラップアラウンド（循環）する。

1つのTCPコネクションを使って送信されるデータは、このようにSYNで始まり、ユーザー・データの1byte目、2byte目、3byte目、……と並び、最後にFINで終了する。オープン時に指定される初期シーケンス番号は、SYNの位置に相当する。

オープン処理では、SYNに対するACKを返しているが、その場合、シーケンス番号に+1したものをACK番号として返しているのはこのような事情による。SYNやFINはTCPヘッダ中に用意された特定のフラグbitであるが、フラグに対する応答を返す手段は用意されていない。そこで便宜的にフラグにもシーケンス番号を割り当てることにより、フラグに対する受信確認を明示的に表現することができるようになっている。



“企業が重視するポイント”に合わせたバックアップソリューションとは

@IT Special

ミドルの転職・AMBIの人気コンテンツ

- PR -



若手7割がスタートアップ転職に意欲 | AMBI (アンビ)



あなたの職務適性が15分でわかる | AMBI (アンビ)



官公庁関連の厳選求人、多数掲載中！「ミドルの転職」

@IT eBook



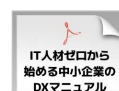
解決！Python CSVファイル編



誰か、要件追加を止めてくれ！——「旭川医大の惨劇」徹底解説



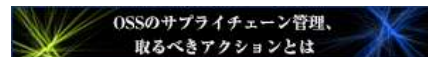
目指せ、共有フォルダ管理の達人！ Windowsファイル共有を“極める”ためのPowerShellコマンドレット基本集



IT人材ゼロでDX! お悩み中小企業のためのDX推進が分かる無料の電子書籍とは

一覧ページへ

注目のテーマ



システム開発ノウハウ【発注ナビ】

- PR -



受託中心の開発会社が『自社サービス』運営に踏み出した理由



スタートアップのシステム会社が4年半で20件以上の新規受注ができた秘訣



受注ゼロから一転、開発会社が2000万円の案件を獲得できた理由

TCP接続のクローズ

次はTCP接続のクローズについてみてみよう。

オープン処理と違って、クローズ処理はやや複雑である。オープン処理のように、3パケット往復するだけですぐにTCP接続が中断・終了されるわけではなく、もう少し緩やかに処理が進められる。上位アプリケーションがTCP接続のクローズ命令を発行しても、すぐにはTCP接続を破棄せず、いくらか待つ必要がある。これには、2つの大きな理由がある。

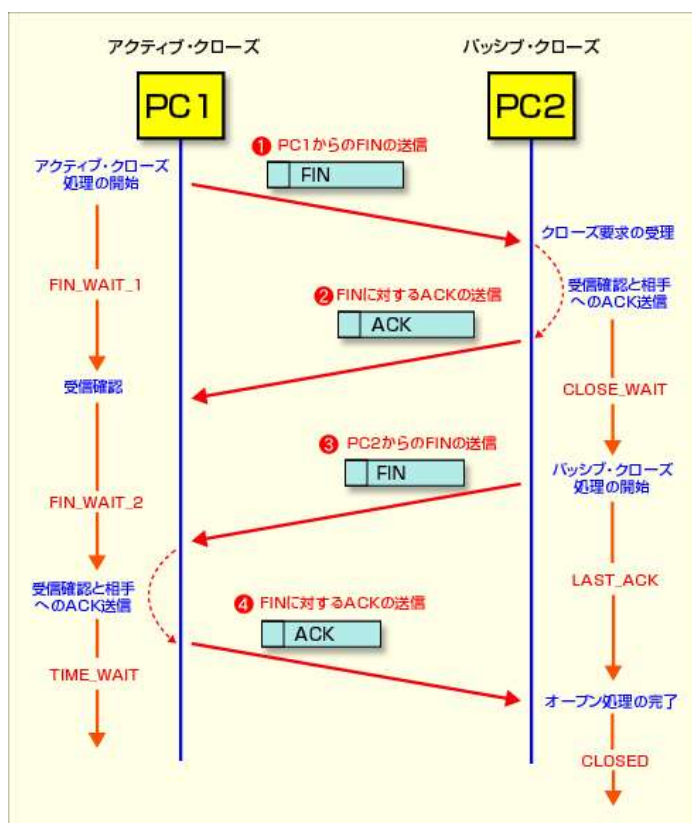
1つは、クローズ処理を始めても、現在送信バッファにデータが残っていれば、それを完全に送信し終わるまでは、TCP接続を勝手に破棄したり、中断したりしてはいけないからである。もし完全にデータを送りきらないうちに（つまり、相手側がデータをすべて受信する前に）TCP接続を終了・破棄してしまうと、最後の部分のデータが相手に届かず、欠けてしまう可能性がある。

もう1つの理由は、上の理由とは逆に、相手からのデータをすべて受信する前に、TCP接続を勝手に破棄したり、中断したりしてはいけないからである。もし完全にデータを受信しないうちに（つまり、相手側がデータをすべて送信する前に）TCP接続を終了・破棄してしまうと、やはり最後の部分のデータが欠けてしまう可能性がある。

このような理由のため、TCP接続のクローズでは、慎重に処理を進める必要がある。具体的には次のような処理が必要になる。

- もし送信すべきデータが残っているのなら、それらをすべて送信し切ってから、送信ストリームのクローズ処理を開始する。送信ストリームの最後にFINを送信すると、それがストリームの終了を表す。
- もし受信すべきデータが残っているのなら（FINの前に何らかのデータあるなら）、それらをすべて受信して、上位のアプリケーションに渡してから、受信ストリームのクローズ処理を開始する。
- 送信ストリームも受信ストリームもともにクローズ処理されると、TCP接続全体がクローズされたものとする。

実際のクローズ処理は、次のようにして行われる。



TCP接続のクローズ処理

クローズ処理では、双方がFINを送信し、それに対するACKの確認が行われる。FINの送信は、もう送信するデータがない、ということ意味する（もうデータを受け取らないという意味ではない）。先のクローズ処理を開始する方をアクティブ・クローズ、そうでない方をパッシブ・クローズというが、オープン処理の場合と違って、クローズ処理は上位アプリケーションからの指示で行われる。

オープン処理と同様に、クローズにも「アクティブ・クローズ」と「パッシブ・クローズ」の2種類がある。先にクローズ処理を行うのが「アクティブ・クローズ」で、後でクローズ処理を行うのが「パッシブ・クローズ」である。両方のクローズ処理が完了した時点でこのTCP接続はすべて終了したとみなされ、プロトコル・スタック内にあるTCP接続に関するリソースなどが解放される。どちらか片方向のストリームが残っている限り、TCP接続はアクティブなままである。

アクティブとパッシブの2種類のクローズ処理は、一見するとオープン処理と同じように見えるかもしれないが、実は大きな違いが1つある。アクティブ・クローズもパッシブ・クローズも、クローズ操作を引き起こす主体（クローズ処理を起動する主体）はそれぞれの上位アプリケーションである。PC1側もPC2側も、もう送信するデータがなくなった時点でクローズ処理を起動している。クローズとは「もう相手からのデータを受け取らない」という意味ではなく、「もうこれ以上送信するデータがない」ということを意味する。そのため、TCP接続の両端のアプリケーションがそれぞれクローズを宣言することにより、初めてTCP接続が終了したと見なされる。

■手順1（（1）、（2））－アクティブ・クローズ

アクティブ・クローズとは、先にクローズ処理を開始することを指す。図からも分かるように、送信するデータの最後にFINフラグ付きのTCPパケットを送り、それに対するACK応答を受け取れば、アクティブ・クローズは完了する。これ以後は、PC1からPC2にもうデータを送ることはできないが、逆にまだ受信することは可能である。

■手順2（（3）、（4））－パッシブ・クローズ

すでに片方向のストリームのクローズ処理が始まった後、逆方向のストリームのクローズ処理を行うことをパッシブ・クローズという。手順1と同様に、送信するべきデータの最後にFINフラグ付きのTCPパケットを送信する。そしてFINに対するACKを受信した時点でPC2からPC1方向のストリームのクローズも終わり、最終的にTCP接続がすべて完了することになる。

以上の手順で分かるように、クローズ処理では、それぞれの方向のストリームのクローズ処理が独立して行われ、両方向とも終了した時点でクローズ処理の完了となる。

[次の回へ >>](#)**インデックス**

「連載 基礎から学ぶWindowsネットワーク ― Windowsネットワーク管理者への道 ―」

[前のページへ](#)[1](#)[2](#)[3](#)

Copyright© Digital Advantage Corp. All Rights Reserved.

- PR -

C-Native
クラウドシフトへの第一歩は、「C-Native」から

伴走型支援
パッケージプラン
短期導入

CTC
C-Native Transformation Service

基礎から学ぶWindowsネットワーク 連載一覧
全 23 回

新しい連載記事が 6 件あります

第17回	LLCとNetBEUIプロトコル
第16回	信頼性のある通信を実現するTCPプロトコル（3）
第15回	信頼性のある通信を実現するTCPプロトコル（2）
第14回	信頼性のある通信を実現するTCPプロトコル（その1）
第13回	データグラム通信を実現するUDPプロトコル

過去の連載記事が 12 件あります

Special

- PR -



「ほとんど誰も見ていない」社内ポータル、どう変えるべき？
New!



「守る」だけでは不十分 今どきのストレージには何が必要？



社内ルールだけでは限界 有名無実化した「ローカル保存禁止」にどう対応？



オンプレのITインフラを「サブスク」で利用できるサービスは何がスゴイのか？



ローコードツールの現在地。AI、機械学習とのシナジーで新たな価値を生み出す **New!**



「ネットワークが分からない」状態からでも丸ごとサポート **New!**



データは「守りながら活用する時代」に



NTTデータと日本IBMがタッグ！ AIは仕事をどう変える？

[@IT Special](#) >

この記事に関連する製品／サービスを比較（キーマンズネット）

- 信頼性や可用性に対する取り組みは？『ネットワークスイッチ』製品比較
- L4負荷分散とL7負荷分散どちらを重視？『ADC／ロードバランサ』製品一覧
- 構築したいネットワーク要件で大きく変わる『ルーター』の選び方
- まずネットワークの性質を十分に見極めよう！『ネットワーク管理』製品比較
- 既存のネットワーク構成とマッチする？『WAN高速化』製品の選び方

印刷

通知

見る

Share

10

@ITについて

お問い合わせ

広告について

採用広告について

利用規約

著作権・リンク・免責事項

サイトマップ

RSSについて

@ITのRSS一覧

アイティメディアIDについて

アイティメディアIDとは

メールマガジン登録

@ITのメールマガジンは、もちろん、すべて無料です。ぜひメールマガジンをご購読ください。

申し込みページへ