

[@IT](#) > [クラウド](#) > [Windows Server Insider](#) > 第18回 NetBIOS over TCP/IPプロトコル（その1）：...

第18回 NetBIOS over TCP/IPプロトコル（その1）

(3/3 ページ)

2004年05月20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

11

前のページへ

1

2

3

NetBIOSのサービスを大きく分けると、名前解決サービス、セッション通信サービス、データグラム通信サービスの3種類がある。前回解説したNetBEUIでは、基本的には1種類のフォーマットの packets でこれらのサービス进行处理していたが、NBTでは、目的別に3種類の異なるフォーマットを採用している。これは、用途に応じて最適化された構造を採用して無駄を省くためであろう。

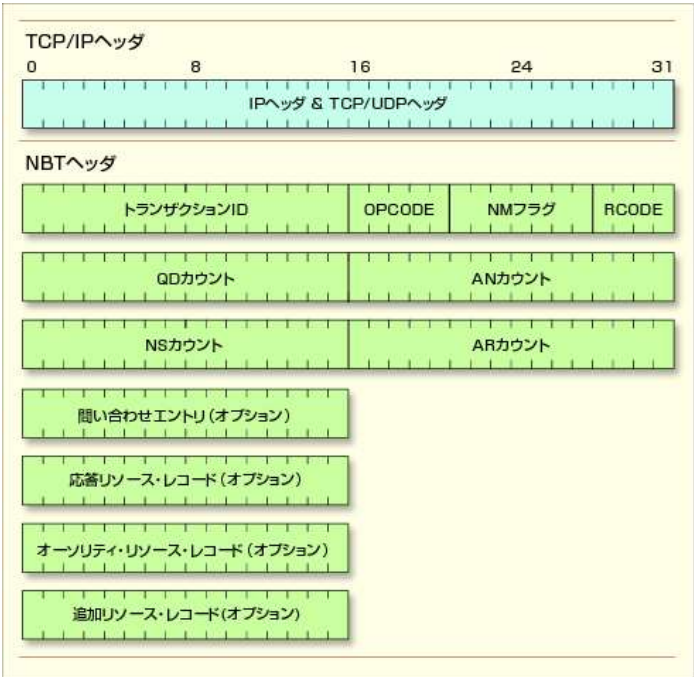
ここでは、これら3種類の packets 構造について解説する。

パケット形式1—名前サービス・パケット

名前サービス・パケットは、NetBIOSによるセッション通信やデータグラム通信に先立って、通信相手を特定するための、問い合わせやその応答に使われる。

すでに何度も述べているように、NetBIOSでは16bytesの「NetBIOS名」を使って通信相手やサービスを特定している。そのため前回解説したNetBEUIの packets 構造でも、送信先や送信元を特定するためにNetBIOS名というフィールドが用意されていた。

だがNBTでは16bytesといった固定長ではなく、ホスト名にドメイン名を追加した、「FQDN名」で通信相手を特定することができるよう仕様が拡張されている。そのため、より長い名前を扱うことができるように packets の構造が可変長となっている。以下にNBTの名前サービスで利用される packets の構造を示しておく。



NetBIOS over TCP/IP（NBT）の名前サービス・パケットの構造
名前サービスでは、NetBEUIの場合と同様に、NetBIOS名の登録や問い合わせ、解放といった処理を行う。NBTではさらに、NetBIOS名からIPアドレスを求めるという処理も担当する。この packets 構造はDNSの問い合わせ／応答 packets と類似している。NetBIOS名前サービスは、TCP／UDPのポート137番を使用する。

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


スポンサーからのお知らせ

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

「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

Special

- 

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？
- 

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？

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!**

これを見ると分かるように、このパケットの構造はNetBEUIの場合とは大きく異なっている。実はこれはDNSの問い合わせ／応答パケットに近い構造になっている（DNSのパケット構造については「RFC1035—DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION」参照）。NBTでは名前の扱いが単なる16bytetsのNetBIOS名ではなく、より汎用性の高いFQDN名となっているため、それに向けたパケット構造として、DNSサービスを参考にして開発されたのだろう。



Special

- PR -

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？

以下、各フィールドについて簡単に説明しておく。

■トランザクションID

これは、名前解決サービスのパケットを識別するために利用される識別番号。名前解決サービスの基本的な動作は、問い合わせパケットの送信と、それに対する応答という形で処理が進むが、どの問い合わせに対する応答であるかを識別するためにこのIDフィールドが利用される。このIDは問い合わせパケットを送信する側でセットし、応答する側では同じIDのまま返信する。こうすることにより、応答が遅れてほかの問い合わせと順番が入れ替わったりしても、正しく送信元のアプリケーションへ応答を返すことができる。

■OPCODE（operation code）

名前解決サービスのコマンド種別を表すコード。同じパケット構造で名前解決サービスに対する要求とその応答を兼用しているため、問い合わせコマンドだけでなく応答に対してもコードが割り当てられている。具体的なOPCODEの値としては次のようなものがある。

数値	OPCODE	意味
0x00	Query	名前の問い合わせ。ある名前がすでにNetBIOS名として登録されているかどうかを問い合わせる
0x05	Registration	名前の登録。コンピュータ名やサービス名、ワークグループ名などを登録するために利用する
0x06	Release	名前の解放。登録したNetBIOS名を解放して、使用を停止する
0x07	WACK（Wait for Acknowledgement）	アクノレッジ（応答確認）を待つ
0x08	Refresh	名前の更新要求
0x09	Alt Refresh	名前の更新要求（正しくは0x08を使うべきだが、RFC文書中のミスタイプにより、この0x09も0x08と同様に扱われる）
0x0F	Multi-Homed Name Registration	マルチホーム・コンピュータにおける名前登録。通常は1つのIPアドレスで1つのNetBIOSコンピュータ名しか登録できないが、マルチホーム・コンピュータでは1つのコンピュータ名で複数のIPアドレスを持つことができる

OPCODEとその意味
5bitsのOPCODEフィールドはNetBIOS名前サービス関連のコマンドの種類を表す。下位4bitがコマンドの種類で、最上位1bitが0ならばコマンド、1ならばその応答を表す。

OPCODEフィールドは5bits幅であるが、最上位の1bitが0ならコマンド、1ならコマンドに対する応答を表し、下位の4bitが実際のコマンド・コードを表す。

■NMフラグ

名前解決サービス用の制御データが格納されたフラグ領域。例えばパケットの送信がブロードキャストかユニキャストかを区別するフラグや、データが規定長を超えたので切り詰められたかどうかを表すフラグなどがある。詳細は省略。

■RCODE（response code）

名前解決サービス・コマンドの実行結果を表すコード。コマンドごとに、その失敗の要因コードが定義されている。



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？



NTTデータと日本IBMがタッグ！AIは仕事をどう変える？



中堅中小企業の“ネットワーク課題”はこれで解決！ New!



「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!



データは「守りながら活用する時代」に



「守る」だけでは不十分 今どきのストレージには何が必要？

@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 -



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？



「守る」だけでは不十分 今どきのストレージには何が必要？

■QDカウント

以下の「問い合わせエントリ」に含まれるレコードの数。

■ANカウント

以下の「応答リソース・レコード」に含まれるレコードの数。

■NSカウント

以下の「オーソリティ・リソース・レコード」に含まれるレコードの数。

■ARカウント

以下の「追加リソース・レコード」に含まれるレコードの数。

■問い合わせエントリ

名前問い合わせにおいて、問い合わせの対象となるNetBIOS名前文字列。

■応答リソース・レコード

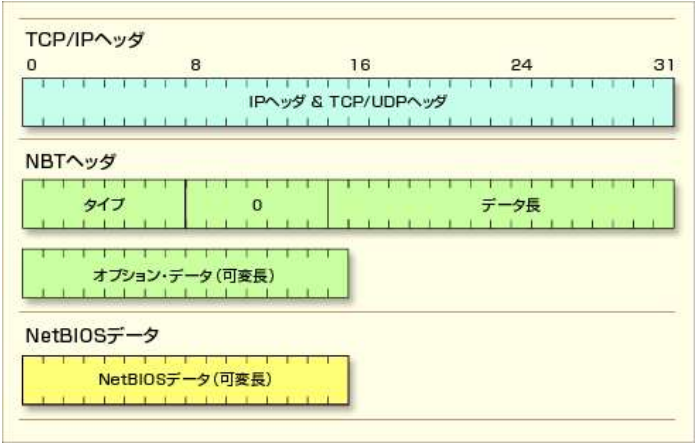
名前問い合わせなどに対する応答のレコード。

■オーソリティ・リソース・レコード／追加リソース・レコード

これらの内容はコマンドに応じて変わる。コマンドごとのパラメータや応答コードなどがセットされる。

パケット形式2—セッション・サービス・パケット

これはセッション指向のデータ通信サービスを行うために利用されるパケットである。一度セッションが確立してしまえば、あとはデータをやりとりするだけなので、パケットの構造は非常に単純である。セッション・サービスでは送信したデータの順序性の維持（送信したとおりにデータが相手に届くこと）やエラー時の再送、通信相手の特定、セッションの維持などの処理が必要になるが、前回解説したLLC+NetBEUIプロトコルと違って、これらはすべて下位のTCPレベルで実現される。そのためNBTヘッダには、ペイロード（データ部分）しか含まれておらず、非常にシンプルになっている。



NetBIOS over TCP/IP（NBT）のセッション・サービス・パケットの構造
セッション・サービスでは、ユーザーのデータをストリームへ送信する。セッション・パケットの信頼性（順序の保証、エラー時の再送など）は下位のTCP層で実現する。NBTのセッション・サービスは、TCPのポート139番を使用する。

以下、簡単に各フィールドについて解説しておく。

■タイプ

セッション通信サービスのコマンド種別を表すコード。具体的には以下のようなコマンドがある。

数値	タイプ	意味
----	-----	----

セッション通信サービスのコマンド一覧

Session Requestでセッションの開始を要求し、認められれば（Positive Session Responseが戻ってきたら）、Session Messageでセッション・データを送信する。



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？

@IT Special

ミドルの転職・AMBIの人気コンテンツ



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）

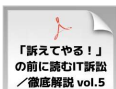


官公庁関連の厳選求人、多数掲載中！「ミドルの転職」

@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



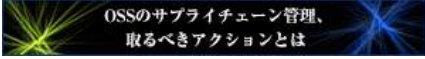
目指せ、共有フォルダ管理の達人！ Windowsファイル共有を“極める”ためのPowerShellコマンドレット基本集



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

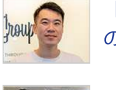
注目のテーマ



システム開発ノウハウ【発注ナビ】



Pythonによるシステム開発でおすすめの開発会社16社



「脱リファラル営業」がエンジニアの実力を高める



Excelではもう限界！2万点以上の在庫管理をシステムで解決

数値	タイプ	意味
0x00	Session Message	メッセージ（セッション・データ）の送信
0x81	Session Request	セッション開始要求
0x82	Positive Session Response	セッション開始要求への肯定応答
0x83	Negative Session Response	セッション開始要求への否定応答
0x84	Retarget Session Response	セッション開始要求へのリダイレクト応答
0x85	Session Keep Alive	セッションのキープアライブ（維持）要求

セッション通信サービスのコマンド一覧
Session Requestでセッションの開始を要求し、認められれば（Positive Session Responseが戻ってきたら）、Session Messageでセッション・データを送信する。

■データ長

NetBIOSデータ部の長さ。最大で64Kbytesまでのデータを送信することができる。

■オプション・データ

コマンドごとのオプション・パラメータのデータ。この部分の詳細はコマンドごとに異なる。例えば「Session Request（セッション開始の要求）」コマンドでは、呼び出す側と呼び出される側のサービスを表すNetBIOS名が含まれるし、「Negative Session Response（セッション開始要求への否定応答）」では、セッション開始要求がエラーとなった原因を表すエラー・コードなどが含まれる。

パケット形式3ーデータグラム・サービス・パケット

これはNetBIOSデータグラム通信サービスのために利用されるパケットである。データグラム通信では、あるひとかたまりのデータ・ブロックを相手に届けるだけであり、エラー発生時の再送処理や送信順序の保証などは行わない。そのため、単にUDPパケット上にデータ・ブロックを載せて、通信の相手先ノードへ届けるだけでよい。データグラム通信の機能や信頼性は、下位のUDPパケット（およびその下位のIPパケット）と同様である。ネットワークの混雑具合によっては、相手に届かないこともあるし、送信した順番どおりに到着しないこともある。

以下にNBTのデータグラム・サービスのパケット構造を示しておく。



NetBIOS over TCP/IP（NBT）のデータグラム・サービス・パケットの構造
データグラム・サービスでは、ユーザーのデータを指定されたあて先へ送信するが、受信確認などは行わない。下位のUDPと同じ程度の信頼性を確保する。NBTのデータグラム・サービスは、UDPのポート138番を使用する。

■タイプ

データグラム通信サービスのコマンド種別を表すコード。具体的には以下のようなコマンドがある。



ページをフォロー



@IT

9時間前

Microsoftは、起業家向けに生成AIを学べるトレーニングコンテンツをMicrosoft Learnで公開した。「アイデア発想」「プロトタイピングとMVP作成」「ビジネスモデル作成」の3つのフェーズで生成AIを活用する方法を学習できる。

数値	タイプ	意味
0x10	Direct Unique Datagram	単一ホストあてのデータグラム送信（ユニキャスト送信）
0x11	Direct Group Datagram	特定のグループあてのデータグラム送信（マルチキャスト送信）
0x12	Broadcast Datagram	データグラムのブロードキャスト（ブロードキャスト送信）。ローカル・ネットワーク上のすべてのコンピュータに対して同報送信する
0x13	Datagram Error	データグラム送信要求に対するエラー応答
0x14	Datagram Query Request	データグラム問い合わせ要求。NetBIOSのデータグラムを中継・展開するサーバ（NBDD：NetBIOS Datagram Distributionサーバ）に対する問い合わせで利用される
0x15	Datagram Positive Query Response	問い合わせ要求に対する肯定応答
0x16	Datagram Negative Query Response	問い合わせ要求に対する否定応答

セッション通信サービスのコマンド一覧
最初の3つのいずれかのコマンドを使ってデータグラム・データを送信する。

以下、簡単に各フィールドについて解説しておく。

■フラグ

各種の制御用フラグ。フラグ中には、NetBIOSのノード・タイプ（次回解説予定）や、データグラムのフラグメント状態を表すF／M（First／More）bitが含まれている。NetBIOSで送信するデータが下位のUDPの制限パケット・サイズを超えるような場合、データをいくつかのデータグラム・パケットに分割して送信する。これをフラグメントという。フラグメント化されたパケットのうち、最初にパケットではF bitを1にして、これが先頭のパケットであることを表す。また最後のパケットでない場合は、M bitを1にして、後続のフラグメント・パケットが存在することを表す。

■データグラムID

送信するデータグラムを識別するための任意のID番号。送信側が任意に割り当てるが、フラグメント化されたパケットでは同一のデータグラムIDを共有し、もともとは同一のデータグラムに属していたことを表す。

■ソースIP

データグラムの送信元IPアドレス。

■ソース・ポート番号

データグラムの送信元のポート番号。

■データグラム長

以下のNetBIOSデータ部分の長さ。

■パケット・オフセット

フラグメント化されたパケットにおいて、データグラムのどの部分のフラグメントであるかを表すために利用される。フラグメント化されていない場合は0となる。

■NetBIOSデータ

データグラムとして送信するデータ。ただし先頭部分には、データグラムの送信元NetBIOS名および先NetBIOS名がエンコードされた状態で格納され、ユーザーのデータはその直後（「パケット・オフセット」の位置）から始まる。ユーザーのデータ（データグラムとして相手に送信されるデータ）は最大で512bytesまでとなっている。

□

今回は、NBTパケットの概要と、パケットの構造について解説した。次回は、より詳細なNetBIOSの通信例や、NBTにおける名前解決の各種の方法について解説する。

[次の回へ >>](#)



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 3 件あります	
第20回	ファイル共有プロトコルSMB／CIFS（その1）
第19回	NetBIOS over TCP/IPプロトコル（その2）
第18回	NetBIOS over TCP/IPプロトコル（その1）
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）
過去の連載記事が 15 件あります	

Special



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？



「守る」だけでは不十分 今どきのストレージには何が必要？



自分が作ったアプリがスマホで動くさまを見ると、学生の目が輝くんです **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？



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!**



「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!**

[@IT Special](#) へ

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）

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

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

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

@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

ITmediaはアイティメディア株式会社の登録商標です。

[メディア一覧](#) | [公式SNS](#) | [広告案内](#) | [お問い合わせ](#) | [プライバシーポリシー](#) | [RSS](#) | [運営会社](#) | [採用情報](#) | [推奨環境](#)