13 用語解説

⑴ IPv6(Internet Protocol version 6)

増加するインターネットの使用者に対応するため、現在の IP（IPv4）に代わるものとして IETF（Internet Engineering Task Force）内の IPNG ワークグループで準備が進められてきたプロトコル。IPv6 には、IP アドレスの 128 ビット化（IPv4 は 32 ビット）、パケットヘッダの簡素化、セキュリティ機能の追加等が盛り込まれている。

⑵ TCP(Transmission Control Protocol)

TCP/IP プロトコルにおける、トランスポート層のプロトコル。2 つのノード上のプロセス（アプリケーション）間で、信頼性のあるセッション指向の通信を行なう。RFC793 等で定義されている。

⑶ STB(Set Top Box)

セットトップボックスの略で、ケーブル TV のコントロールボックスや、通信カラオケの端末機器等、家庭用テレビに接続して追加機能を提供するデバイスの一般名称。通常、TV の上に置くことからこのように呼ばれる。次世代の家庭用情報サービスとして注目される、ビデオ・オンデマンドやインタラクティブ TV 等を可能にするセットトップボックスが現在注目を集めている。

⑷ DV(Digital Video)

家庭用デジタルビデオのこと。

⑸ PeerToPeer

コンピュータ同士を直接接続して、お互いの持つ情報をやり取りする通信形式。

⑹ IPv4(Internet Protocol Version 4)

現在のインターネットで利用されているインターネットプロトコル(IP)。アドレス資源を 32 ビットで管理しているため、識別できるコンピュータの最大数は 42 億 9496 万 7296 台である。しかし、近年のインターネットの急速な普及により、アドレス資源の枯渇が予想以上に早く生じるとの危惧が関係者の間に高まり、128 ビットでアドレスを管理する IPv6 が開発された。

⑺ グローバルアドレス

インターネットの IP アドレス(IP プロトコルで使用するための 32bit のアド

レス情報)空間。インターネットでは、特定の IP アドレスから、一意に特定のノードを決定できることからこのように呼ばれる。

⑻　プライベートアドレス

　インターネットへの接続が必要ではないネットワークアドレスとして自由に利用できる IP アドレスのこと。Class A 10.0.0.0～10.255.255.255、Class B 172.16.0.0～172.31.255.255、Class C 192.168.0.0～192.168.255.255 が規定されている。

⑼　NAT(Network Address Translation)

閉じられたネットワーク環境内で通用するプライベート IP アドレスと、インターネットアクセスに利用できる本来のグローバルな IP アドレスを相互に変換し、ローカルな IP アドレスしか割り当てられていないノードから、透過的にインターネットをアクセスできるようにする技術。

⑽　IP マスカレード(IP masquerade)

NAT による IP アドレスの変換だけでなく、その上位プロトコルである TCP／UDP のポート番号も識別することで、異なる通信ポートを利用するものについては、1 つのグローバル IP アドレスを利用して、複数のローカルノードが外部と通信できるようにしたソフトウェア。UNIX システムの 1 つである Linux 上で最初に開発された。

⑾　プロキシサーバ(proxy server)

ファイア・ウォールの内側にあるクライアントからアクセス要求（HTTP、FTP 等）を受け付け、クライアントの代理を務めるサーバの総称。これによって、ファイア・ウォールを超えて外部にアクセスすることができる。プロキシサーバは自分のディスクに取得したデータをキャッシュするため、同一ファイルがアクセスされた場合にはキャッシュされたファイルを転送してスピードの向上にも貢献する。

⑿　UDP (USER DATAGRAM PROTOCOLUser Datagram Protocol)

インターネットでは、トランスポート層のプロトコルとして TCP も使われるが、UDP のほうが転送速度が高い。しかし、TCP のようにデータが相手に到着したかどうかの確認を行わないため、信頼性が低いというデメリットもある。一般にストリーミング等に使われる。

⑴3⑵ FTTH(Fiber To The Home)

電話局から各家庭までの加入者線を結ぶアクセス網を光ファイバ化し、高速な通信環境。

⑴4⑵ JGN (Japan Gigabit Network)

超高速ネットワーク技術や高度アプリケーション技術等、情報通信技術の水準向上に寄与することを目的に、通信・放送機構（TAO）が、日本初の本格的な次世代インターネットのための研究開発用テストベッドとして、平成 11 年 4 月から運用を開始し、大学、研究機関、行政機関、地方自治体、企業等に研究開発用として広く開放され、利用者を限定しないオープンなネットワークとして活用された。

⑴5⑵ NetMeeting®

Microsoft 社が無償提供する電子会議ソフト。リアルタイムチャット、ホワイトボード機能 、ヴォイスチャット 、ビデオ機能、ファイル送受信、アプリケーションの共有等の機能がある。

⑴6⑵ MPEG2

動画を圧縮するための技術で､DVD ビデオに適用されている MPEG2 は 720×480 ドットの画像を 1 秒間に 30 コマ表示する。高画質で DVD ビデオだけでなくデジタル衛星放送にも利用されている。

⑴7⑵ H.323

テレビ電話等の実装に利用され、ネットワーク上で音声・動画を 1 対 1 で送受信するために音声、映像方式、データ圧縮伸長方式等を定めたプロトコル。

⑴8⑵ SIP(Session Initiation Protocol)

VoIP(Voice over IP :IP ネットワーク上で音声通話を実現する技術。)を応用したインターネット電話等で用いられる、通話制御プロトコルの一つ。1999 年 3 月に発表された規格で、転送機能や発信者番号通知機能等、同様のプロトコルと比べて公衆電話網に近い機能を備え、接続にかかる時間も短くなっている。また、各端末に割り当てられるアドレス形式が電子メールアドレスの形式に近く、将来的には共通化も可能とされている。

⑴9⑵ DVcommXP

ファットウェア社が開発したソフトウェアで､WindowsXP 上で稼動しホームビ

デオや業務用ビデオとして採用されている DV(デジタル・ビデオ)規格の高画質映像とステレオ音声を、ブロードバンド・ネットワーク経由で伝送できる。

⑳ DVTS(Digital Video Transport System)

高品質動画像を送受信するシステム。 30Mbps の帯域を利用し、テレビと同等の品質が実現できるフリーソフト。FreeBSD、 Linux、 MacOS X、 NetBSD、 Windows2000、 WindowsXP 等の基本ソフトに対応。

㉑ VPN (Virtual Private Network)

インターネットを経由するにもかかわらず、拠点間を専用線のように相互に接続し、安全な通信を可能にするセキュリティ技術。「仮想専用線」「仮想私設網」等と呼ばれる。コストのかかる専用線の代替になる新しいインフラとして、企業を中心に着実に浸透している。VPN を利用した通信を行なうには、接続点に VPN 機能を備えた専用装置（以下、VPN 装置）が必要だが、最近ではルータやファイア・ウォールにその機能が含まれるものも多い。

㉒ トンネリング(tunneling)

あるプロトコルパケット A を別のプロトコルパケット B でカプセル化して、プロトコル B での通信を行ない、通信を外部から隠蔽すること機能をもつ。

㉓ 中継点オプションヘッダ

中継点オプションヘッダは、パケットの配達経路に沿ってすべてのノードにより調査されなければならないオプションの情報を伝えるために使用される。中継点オプションヘッダは IPv6 ヘッダにおいて次ヘッダを示す値である 0 により識別される。

㉔ 経路制御ヘッダ

経路制御ヘッダは、パケットの終点までの途中で訪問されるための 1 つ以上の中間ノードをリストするために、IPv6 始点によって用いられる。経路制御ヘッダは、直前のヘッダの次ヘッダ値 43 によって識別されている。

㉕ IPComp

IP パケットのトランスポート層を圧縮するプロトコルである。 IPComp を IPsec の ESP と組み合わせることによって、 VPN のスループットを向上できる可能性がある。特に、低速な回線では、スループットに対するデータ量の影響が大きいため、IPComp は効果的に機能する。

⑵⑹ マルチキャスト(multi-cast)

パケット通信技術の 1 つ。単一のパケットで、複数のノードに対して同一データを送信する通信方法をマルチキャストと呼ぶ。マルチキャストに対して、ネットワーク内の全ノードに対して送信する方法はブロードキャストと呼ばれる。

⑵⑺ IKE(Internet Key Exchange)

IPsec においてホスト間で SA を確立する時毎に管理者が手動で鍵の設定を行うのではなく、動的に鍵情報等をホスト間で安全に交換するための鍵管理プロトコル。IPsec は鍵交換が行われて初めて有効となるため、IKE 自身の通信を保護するために、IPsec で確立される SA 以外に、独自の SA を生成する。

⑵⑻ DoS 攻撃(Denial of Services attack)

日本語では「サービス拒否攻撃」。Web サイト等に対して、限度を超えた多量のアクセスを与えることで、回線容量やサーバの処理能力をパンクさせ、本来のサービスをできなくするクラッカーの常套手段。

⑵⑼ PKI (Public Key Infrastructure)

公開鍵暗号技術と電子署名を使って、インターネット上で安全な通信ができるようになりすましやデータの盗聴や改竄を防ぐための環境のこと言う。公開鍵暗号技術とは、暗号化と復号化で一対の異なる鍵を利用する方法で、片方の鍵で暗号化された情報はそれと対になっているもう一方の鍵でなければ復号化できない。例えば A が B に文書を送る場合、A は B の公開鍵を入手し、その公開鍵で文書を暗号化する。B は自分の秘密鍵(B しか持っていない)を使用して文書を復号化し、文書を読むことができる。この公開鍵・秘密鍵は認証局が本人確認の上、電子証明書とともに発行するものである。電子証明書とともに文書を送ることで、通信相手の正当性を確認することができる。