



最初の30問は、5ジャンルの「素朴な疑問」のなかでも特に初心者向けのテーマを選んだ。LAN・無線LANのジャンルから「IPv4アドレスには、なぜグローバルとプライベートがあるの?」といったテーマを取り上げた。WAN・モバイルのジャンルでは、「spモードってiモードとどう違うの?」などの疑問を選んだ。Web・クラウドは「IPv4グローバルアドレスは、もう完全になくなっちゃった?」、セキュリティは「ウイルスや攻撃の名前はどやって付ける?」、法律・制度・標準は「技適って何?」「自炊代行は違法なの?」など、今どきのテーマを取り上げた。

☛が付いている用語は pp.66-67 でまとめて解説してある

001 IPv4アドレスには、なぜグローバルとプライベートがあるの?

IPv4☛アドレスにグローバルとプライベートがあるのは、実はIPv4アドレスの枯渇に大きくかかわっている。

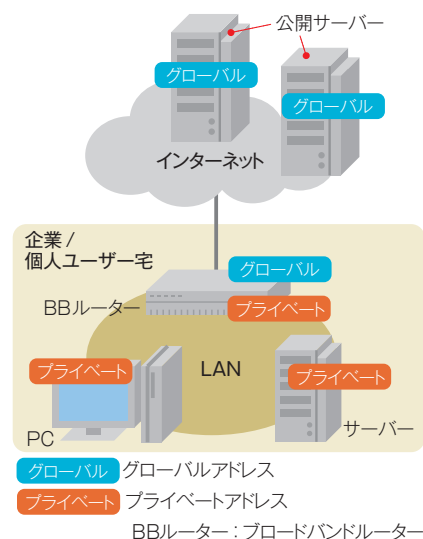
そもそもIP☛は、インターネットでデータをやり取りするための最も基本的なプロトコル☛。IPには現在主に使われているIPv4と、使われ始めたIPv6☛という二つのバージョンがある。IPでは、すべてのデータをIPパケット☛という形式でやり取りする。IPパケットを届ける宛先を指定するのに使うのがIPアドレスであり、そのIPv4バージョンがIPv4アドレスだ。

インターネット上では、宛先を区別できるように、各端末に重複しないアド

レスを割り当てる必要がある。ところが、32ビット長のIPv4アドレスで重複せずに作れるアドレス数は約43億個であり、1990年代には、早晚枯渇してしまうことが明らかになった。

そこで、約43億個のIPv4アドレスのうち、インターネット上で使うグローバルアドレスとは別に、インターネットと直接接しないLANの内部で使うためのプライベートアドレスを定義した。プライベートアドレスはインターネット上の端末には使えないが、その代わりに、異なるLANで重複して使える。さらに、LAN内の複数のプライベートアドレスから、1個のグ

ローバルアドレスを使えるようにするNAPT☛という仕組みも作られた。



002 公衆電話の場所を公開するようになったのはなぜ?

NTT東日本とNTT西日本(NTT東西)はこれまで、公衆電話の場所を一般には公開してこなかった。理由の一つは、中にたまったお金の盗難を防止するため。町中に数多くあるのであえて場所を公開しなくても不便ではないだろうという考えもあった。

こうした方針を変えるきっかけが、2011年3月11日に起こった東日本大

震災だ。公衆電話には、災害の輻輳時にも通話が優先されたり、局側からの給電で停電時に使えたりといった特徴があるため、東日本大震災で重要な通信インフラとして再認識された。

そこで、災害時に公衆電話の場所がすぐにわかるように、その位置を公開することになった。公開時期は「平成24年度のできるだけ早いうち」(NTT

東日本)。平成24年度が始まる2012年4月から数カ月を念頭に置いている。

公開する形式としては、ユーザーの利便性を考慮しWeb上の地図で位置を示す形にする。同社はまず自社のWebサイトで地図を公開。さらに、各自治体の防災マップや様々な地図サービスに掲載できるように、積極的に協力していくという。

003 MACアドレスとIPアドレスの両方が必要なのはなぜ？

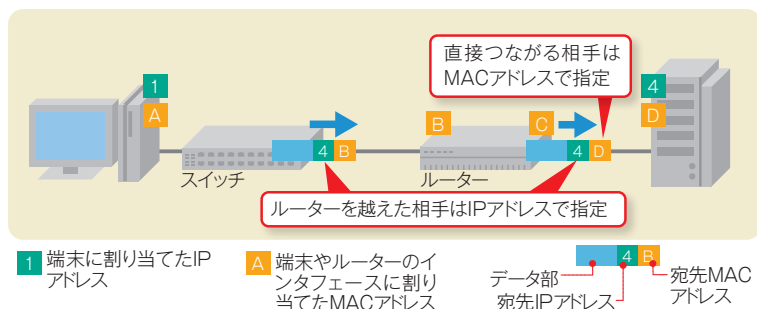
コストを度外視すれば、MAC^{マック}アドレスだけでインターネットのようなグローバルネットワークを構築することは可能である。しかし、実際のLANやインターネットでは、MACアドレスとIP^{アイピー}アドレスを連携させて機能するようにプロトコル^{プロトコル}が設計されており、それぞれを省くことは不可能となっている。こうした状況に至るまでには、歴史的な経緯がある。

IPはもともと、異なるプロトコルで動作するLANや広域ネットワークを相互接続し、一つのネットワークとして束ねるために作られた。その「ネットワークのネットワーク」で宛先を一意に決めるために定義したのがIPアドレスだ。IPアドレスはネットワークを示す部分とホストを示す部分に構造化され、柔軟に設定可能となっている。こ

れによりアドレスを集約してルーターに登録する経路情報を大幅に減らせる。

一方のイーサネットは、当初は短距離・小規模のLANで、高速伝送を安価に実現するために開発された。ここでは端末を一意に識別するMACアドレスを定義する。短距離の高速伝送に向くイーサネットと、それらを数珠のようにつないでグローバルネットワークを構成するIPが、補完し合って現在のインターネットが発展した。

冒頭で述べたように、MACアドレスだけでグローバルネットワークを構築するとどうなるだろうか。MACアドレスはIPアドレスのように集約できない。端末数が膨大になると、経路を蓄えるメモリー量や経路探索の処理量が莫大となり、スイッチを現実的なコストで製造するのは不可能だろう。



005 標準が決まるまでなぜ何年もかかる？

新しい規格（標準）に対応した製品が販売されるとき、まだその規格の標準化が完了していないことがある。そうした状況は無線LAN製品でよく見られる。無線LAN規格の標準化作業に参加しているNTT未来ネット研究所の浅井 裕介^{あさい ゆうすけ}氏によると、標準化に時間がかかる要因は二つ考えられるという。一つは合意形成に時間がかかることだ。標準化の目的の一つは、製品の互換性を確保すること。標準化作業に参加す

る企業は、開発コストなどを考慮して自社にとって作りやすい規格になるように技術提案をするため、意見調整に時間がかかる。もう一つの要因は、既存規格との整合性をとるための確認作業に時間がかかること。LAN技術に関するIEEE 802標準の場合、規格の下書きを参加者全員でレビューし、寄せられたコメントを一つずつすべて処理しなくてはならない。11nではこの作業に3年以上もかかったという。

004 無線LANの電波はどこまで飛ぶ？

電波自体は理論上、無限に届く。しかし、“無線LANの電波”といった場合、データを乗せた意味のある信号として受信側に届くという意味になる。こうなると、その届く範囲は限られる。

無線LAN機器は、一定の条件を満たすことで免許を受けずに利用できる特定小電力無線局である。この条件の一つとして、送信出力が10mW以下と法令で定められている。一般的に、こうした条件で無線LANの電波が届くのは数十mといわれている。

ただし、同じ送信出力でも、指向性を持つアンテナを使って特定の方向だけに電波が飛ぶようにすれば、より遠くまで届く。企業向けの外付け指向性アンテナでは、数km程度まで距離を延ばせるとうたっている製品が多い。^{アイトリプルイー}このほか、IEEE 802.11n対応の一部の製品でも、ビームフォーミング^{ビームフォーミング}と呼ぶ機能で、電波が届く範囲を1.5～2倍程度に延長するものがある。

006 匿名サイトの投稿者はどうやって特定する？

2010年11月の尖閣諸島沖漁船衝突映像の流出や、2011年2月に発覚した質問掲示板を使った大学入試のカンニングでは、匿名サイトへの投稿にもかかわらず、利用したネットカフェや携帯電話が比較的早く特定された。その理由は投稿者のIP^{アイピー}アドレスだ。匿名サイトでも通信時には必ずIPアドレスを使うため、それを基に送信元を突き止められる。ほとんどのサービスは投稿者のIPアドレスを一定期間保持しており、法的に正当な請求があれば開示する。IPアドレスからプロバイダーがわかれば、その発信場所や契約者情報なども、同様に開示請求できる。

007 有線LANで給電できるんだから、無線LANで給電できないの？

LANケーブルで電気を供給するPoE^①はあるが、現時点では無線LAN(2.4GHz帯、5GHz帯)による給電は実用化していない。

無線LAN以外の「ワイヤレス給電」は既にある。飛距離があまりないので「ワイヤレス感」がないが、NTTドコモの携帯電話の「おくだけ充電」などだ。YRP研究開発推進協会 研究企画部長 ^{かじわら りょう} 梶原 亮氏によると、携帯電話のワ

イヤレス給電には「電磁誘導方式」(送電側と受電側の間で発生する誘導磁束を利用して電力を送る方式)が適用されているが、今後は長距離・大電力の「磁界・電界共鳴方式」(離れた距離でも共鳴現象で送電する方式)や「電波発射方式」(アンテナで発射した電波を電力として受信する方式)も期待されている。「ただし電波発射方式は電磁誘導方式より伝送効率が悪いため、実用

化には時間を要するだろう」という。

一方、“勝手に電波を電力に変換する方式”もある。米パワーキャストは、電波を受信してそこから電力を引き出すチップを製造している。ただし「周囲の条件にもよるが、現時点では2～3ミリW程度しか取り出せないため用途は限定的だ」(チップの販売代理店である東京エレクトロン ^{しんたに こうぞう} デバイスの新谷 浩造氏)という。

008 Androidのアプリって安全じゃないの？

米グーグルによるAndroidマーケット(現Google Play)には、不正な動作をするアプリが混入する可能性があるという話を聞く。これには、Androidアプリを公開する前に審査を実施する仕組みがなく、自由に配布できることが背景にある。一方iPhoneやiPad用 ^{アイフォーン アイパッド} のApp Storeでは、アプリを公開する前に審査があるので、そうした被害はあまり聞かない。

KDDIはこうした問題から、Android

アプリ配布サイトとして「auスマートパス」を利用した「アプリ取り放題」を2012年3月1日から始めた。このサービスでは、同社がアプリの配布前にウイルスが混入していないかどうかなどをチェックする。チェックしたアプリはプログラムごと同社の配布サーバーに保存され、そこからユーザーがダウンロードする仕組みだ。他社の配布サイトではGoogle Playへのリンクだけを提供しているものもあるが、「アプリ取り放題」ではアプリがバージョンアップしたときでもその都度KDDIがチェックしているので安心度が高い。

なお、アプリが端末上のどの情報に

アクセスして外部に送信しているかは、配布サイト上のアプリの詳細情報や、インストール後のアプリの詳細情報でもわかる(図)。



009 Webを考えたのは誰？

Webを考えたのは、欧州のCERN ^{セルン}で働いていたティム・バーナーズ＝リー氏だ。もともとはCERNの情報管理システムを構築する技術としてWebを考案。Webを構成する基本的な仕組みであるHTTP^②とURI^③、HTML^④をすべて開発した。1990年末には最初の、基本的な三つのWebブラウザとWebサーバーを完成させた。CERNは同氏からの要望を受け入れる形で、Web技術を完全に付帯条件なしで使える“パブリックドメイン”にすることを宣言した。1995年には、Web技術の標準化団体であるWorld Wide Webコンソーシアム(W3C^⑤)が設立された。

010 IPv6インターネットを使ってみないけど、どうすればいい？

IPv6^⑥インターネットにつなぐには、何らかの接続サービスに加入しなくてはならない。様々な接続サービスがあるが、大きくは「既存のIPv4^⑦インターネット接続を生かして、IPv6インターネットにもつないでくれるもの」と、「純粋にIPv6インターネットに接続するもの」に分けられる。前者のタイプの主流は、IPv6のパケットをIPv4のパケットで包み込み、IPv6インター

ネットの入り口まで運ぶ「トンネリング」という仕組みを使う。通信事業者の一部やOSベンダー、有志によるプロジェクトがトンネリング技術を使ったサービスを提供している。後者のタイプはIPv4インターネット接続とIPv6インターネット接続をセットで提供する「デュアルスタック」というサービスが主である。これらのサービスも、既に一部の通信事業者が提供中だ。

011 2.4GHz帯の無線LANと5GHz帯の無線LANはどこが違う？

無線LANで利用できる周波数帯は、2.4GHz帯と5GHz帯の二つに分けられる。両者は、使用できる規格や場所、チャンネル数、他の用途との共用、対応機器の数などの点で違いがある。

使用できる無線LAN規格でみると、2.4GHz帯はIEEE 802.11、802.11b/g/nだ。5GHz帯は802.11a/nで、2012～2013年には802.11acが加わる。

使用できる場所は、5GHz帯の方が厳しい条件が付く。2.4GHz帯は屋外でも屋内でも使えるが、5GHz帯はW56と呼ばれる周波数帯だけが屋外・屋内両用。W52およびW53と呼ばれる周波数帯は屋内専用だ。

チャンネル数は5GHz帯が19で、2.4GHz帯の13より多い。2.4GHz帯は隣接するチャンネルと一部使用周波数帯が重なる。5GHz帯はW53とW56の間に無線LANで使えない周波数帯があり、

チャンネルが二つの固まりに分かれる。

周波数帯を共用する他の用途は、2.4GHz帯のほうが多い。2.4GHz帯は広範な用途を持つISMバンドであるため、無線LAN同士だけではなく、医療機器や電子レンジなどとの間でも電波干渉が起こり得る。5GHz帯は、W53/W56で気象レーダーなどが一定以上の強さの電波を出していると自動的に別のチャンネルに切り替える仕組みがある。

対応機器の数は2.4GHz帯が5GHz帯を圧倒的に上回る。特にスマートフォンやポータブルゲーム機は、2.4GHz帯だけしか使えないものが大半だ。

無線LAN機器メーカーのパッファロ

ーは、2.4GHz帯は手軽に使えるメリットはあるが、かなりの混み具合になっていることがありパフォーマンスでは5GHz帯に一步譲る部分があると指摘。「スマートフォンやタブレット端末などでTwitterやメールをする程度であれば2.4GHz帯でも十分だが、接続の安定性と高速性が求められる映像視聴やオンラインゲームなどでは、5GHz帯に利があるだろう」と説明する。

	2.4GHz帯	5GHz帯
使用できる通信規格	IEEE 802.11、11b、11g、11n	IEEE 802.11a、11n、11ac (2012～2013年頃に使われ始める見込み)
利用できるチャンネル数	13チャンネル(隣接チャンネルと重複する)	19チャンネル
他用途の電波との共用	ISMバンドであり、医療、産業、科学分野の機器と共用。電波干渉が起こり得る	W53とW56は気象レーダーなどと共用。衛星やレーダーが電波を出している帯域は使えない
使用可能な場所	屋外、屋内とも使用可能	W52、W53は屋内専用。W56は屋外・屋内両用
対応機器の数	5GHz帯より多い	2.4GHz帯より少ない

012 PAN/LAN/MAN/WANはどの範囲のネットワーク？

千葉大学大学院 融合科学研究科情報科学専攻 情報通信ネットワークの阪田史郎教授は、「PAN/LAN/MAN/WANは無線ネットワークでの定義を覚えるとよい」とアドバイスする。有線はLANとWANだけで、定義も無線と違うからだ。

無線でのPAN/LAN/MAN/WANは、使う技術で分ける。PANはアクセスポイントからの通信距離が最大で10～20mのネットワークで、IEEE 802.15で定められた技術を使う。「Bluetooth/Zigbee/UWB、可視光通信、BANなどだ」(阪田教授)。似た通信距離を持つNFCやRFID、TransferJet、特定小電力無線などは短距離無線という。PANはn:n、短距離無線は1:1で通信する点が違う。

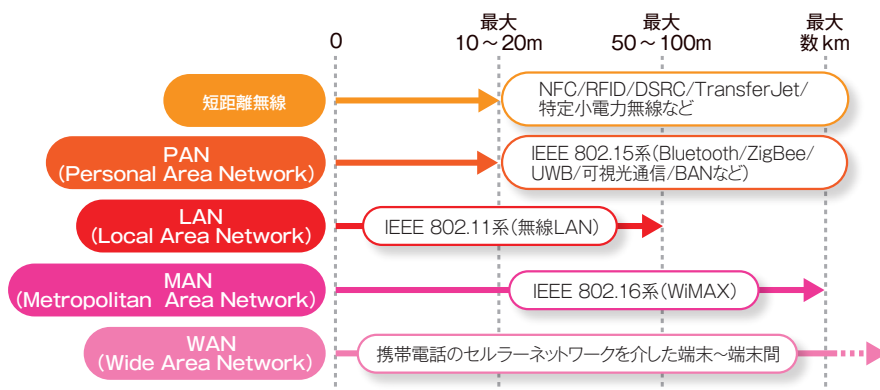
LANは、IEEE 802.11として標準化された無線LANである。標準化中の802.11adは通信距離が短くPANに見えるが、「規格は802.11として定められるためLANに分類する」(同氏)。

次に、WANを先に見ておこう。WANは携帯電話のセルラーネットワークを含む、通信する端末間のネッ

トワークである。

最後にMANは、基地局からの通信距離が最大数kmのネットワークで、技術はIEEE 802.16のWiMAXだ。ただ802.16mは4G(第4世代携帯電話)の一つに数えられ、長期的にみるとMANはWANに収束されていくのではないかと阪田教授はみている。

無線におけるPAN/LAN/MAN/WANと通信距離の関係



013 スпамは減っている? 増えている?

スパム対策は、企業でも個人でも一般的なセキュリティ対策となった。では、スパムメールの数は今も増えているのか。あるいは減ってきているのか。

スパム対策の製品やサービスを持っているセキュリティベンダーに聞いた結果を総合すると、「スパムは依然多いが、一時期よりは減ってきている」という傾向がみえてくる。

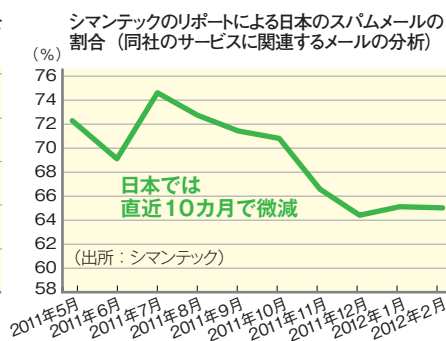
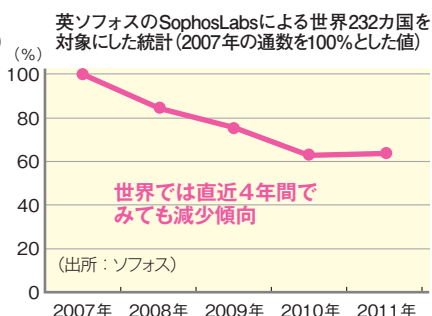
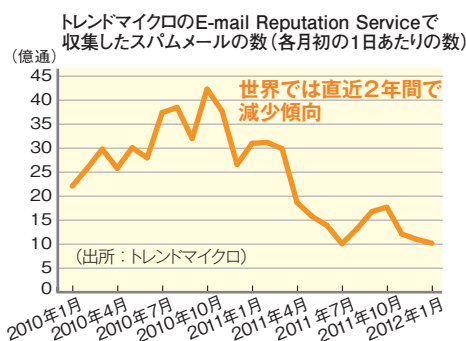
左のグラフは、トレンドマイクロの

E-mail Reputation Serviceで収集したワールドワイドでのスパムメール数の増減傾向を示したもの。直近2年間でみると減少傾向にある。真ん中のグラフは、英ソフォスのラボにおけるワールドワイドでの統計だ。2007年を100%とすると、2011年には63%まで減っている。そして右のグラフは、シマンテックが日本におけるスパムメールの割合を分析したもの。2011年5月

～2012年2月のデータだが、激増した痕跡はない。トレンドマイクロは、「2011年春頃に落ち込んだのは、Rustockというボットネットの閉鎖によるものと見られる」と説明する。

だが、「スパムが減ったのでひと安心」とはいえない。ソフォスは、「ここ数年スパムメールは減少傾向にあるが、引き換えにマルウェアに感染したサイトが増えている」と警告する。

セキュリティベンダーが出している統計データからスパムメールの増減傾向を読み解く



014 技適って何?

スマートフォンを含む携帯電話機について「技適を通っている」「技適マークが付いた」などというのを聞いたことがあるかもしれない。「技適」とは何なのだろうか。

発売される携帯電話機やスマートフォンは、法律で定める審査を通して技術的に基準を満たしているという証明・認定を受け、それを通ったことを示すマークを付けるか表示することを定めている。具体的には、電気通信事業法による「技術基準適合認定」と電波法による「技術基準適合証明」の2種類である。「前者は公衆ネットワークにつながるため、後者は電波を出すためのもので、携帯電話機の場合は両方が必要だ」(電気通信端末機器審査協会(JATE)機器審査部 主幹の寺田 昭彦氏)。技適は正式な言い方ではなく、携帯電話機の場合

はこれら2種類の審査のことを指すと考えればよい。携帯モデムがなく無線LANでしかつながない携帯端末でも、2種類の審査を通す必要がある。

携帯電話機の場合、認定・証明されたことを表すマークの横には四角で囲ったTとRの文字および番号が併記される。Tが電気通信事業法、Rが電波法のものである。JATEの寺田氏は「従来は端末のどこかにマークが付いていたが、2011年4月から画面表示の形でもよくなった」と説明する。iPhone/ iPadは画面でマークを見られる。認定機関はTマークの方がJATEなど、Rマークの方がテレコムエンジニアリングセンターなどである。



015 IEEEとIETFの違いは何?

本誌には、IEEEやIETFで標準化された技術の話題がよく登場する。両者の違いを知っておこう。

IEEEはInstitute of Electrical and Electronics Engineersの略で、米国電気電子技術者協会と訳す。米国に本拠を置く電気・電子関連の学会だが、ネットワーク関連では「802委員会(IEEE 802 LAN/MAN Standards Committee)」で、主にLANで使う規格の標準化作業をしている。IEEE 802.3のイーサネット、同802.11の無線LANなどがある。IETFはInternet Engineering Task Forceのこと。インターネットの標準規格を記した技術文書「RFC」の発行団体だ。IPやTCP/UDP、その上位プロトコルは、RFCで仕様が決められている。

016

spモードってiモードとどう違うの？

spモードとiモードはいずれもNTTドコモが提供する携帯電話向けインターネット接続サービス。違いは利用できる端末のタイプにある。spモードはスマートフォン、iモードはフィーチャーフォン(iモード端末)である。ちなみにspモードの「sp」はsmartphoneから音節の頭文字をとったもの。

もともとspモードは、スマートフォンでiモードと同じメールアドレス(docomo.ne.jpドメイン)を使えるサービスとして2010年8月に始まった。メール、インターネット接続、コンテンツ決済の三つが基本サービスである。

オプションとしてメールのウイルスチェックとサイトのフィルタリングサービスが用意された。その後、iチャネルやiモードサイトなどiモード独自のサービス/コンテンツのスマートフォン

ン対応が進み、iモードから見たspモードとの差は小さくなっている。今後も「iモードで提供しているサービスは基本的にspモードでも使えるようにする」(NTTドコモ)という。

	spモード	iモード
サービスの定義	スマートフォン向けインターネット接続サービス	フィーチャーフォン(iモード端末)向けインターネット接続サービス
主なサービス	メール	spモードメール(@docomo.ne.jpを利用)
	サイト閲覧(ブラウザ)	iモードメール(@docomo.ne.jpを利用)
	コンテンツ決済	iモードサイト(iモードブラウザ)、Webサイト(フルブラウザ)
サービスの提供基盤	CiRCUS/MAPS	CiRCUS

CiRCUS : treasure Casket of i-mode service, high Reliability platform for CUSomer
MAPS : Multi Access Platform System

017

ワイヤレス給電って人体への影響はないの？

影響がないとは言い切れない。ワイヤレス給電は磁界や電界、電磁波を使って電力を送る。日本では磁界、電界、電磁波の強度に関する一種のガイドラインとして総務省が定めた「電波防護指針」がある。「人体への影響を考慮して作られたもので、ワイヤレス給電の場合も指針で示される値以下で使用する必要がある」(東京大学 新領域創成科学研究科先端エネルギー工学専攻^{いむら たけひろ}の居村 岳広助教)

ただし、ガイドラインを守った製品でも人体への影響が出てくるケースがある。スマートフォンを含む携帯電話機やタブレット端末向けのワイヤレス給電製品では、取り扱い説明書に「心臓用ペースメーカーや除細動器を装着している場合は、製品の使用に当たって医師とよく相談してください」といった警告表示がある。説明書における警告とは、「取り扱いを誤った場合、死亡または重症を負う可能性が想定され

る」というものだ。

このほかにも、充電台に異物があると発熱してやけどの原因になることがある。「クリップや硬貨などの金属片を挟まない」「給電装置をアルミなどのシールや金属製のものを貼り付けない」といった警告が示されている。製品は異物を感知する仕組みを備えているが、100%検知できるわけではないので、このような警告がなされているというわけだ。

018

固定電話がなくなるって本当？

なくなるのはPSTN[☎](Public Switched Telephone Networks)。これはIP[📶]が登場する以前の技術により、一般加入電話サービスなどを提供している電話網である。

NTT東西は2010年11月、PSTNからIP網への移行(マイグレーション)を発表。2020年頃に開始し、2025年頃の完了を予定している。PSTNマイグレーションでは、PSTNにより提供しているサービスを終了し、加入者交

換機などを撤去する。提供中のサービスは、引き続きIP技術などにより提供を継続するものと終了するものがある。継続するサービスには基本的な音声サービスがある。このほか、公衆電話や緊急通報、発信者番号通知など18のサービスを継続する。終了するサービスはマイグレーションと同時に終了するものと、マイグレーションに先立って終了するものがある。同時に終了するサービスはINSネット(ISDN)やピ

ンク電話、短縮ダイヤルなど19のサービス。マイグレーションに先立って終了するサービスは16ある。このうちダイヤルQ²とネーム・ディスプレイについては既に新規申し込み受付を終了しており、サービス提供の終了時期も発表されている。

なお、他の終了予定サービスについては「必要に応じて、代替サービスの提案を行っていく」(NTT東日本)という。

019

カテゴリ3のケーブルを100Mイーサに使ったらどうなる?

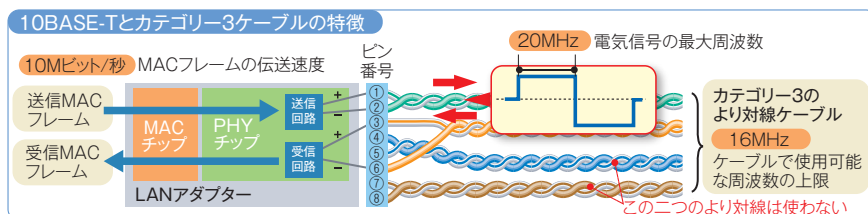
ケーブルが短ければ問題なく通信できるケースもあるが、長くなるほど通信は不安定になる。

カテゴリはより対線のLANケーブルの分類。カテゴリ3は伝送規格は10BASE-T対応で、最大伝送速度は10Mビット/秒だ(図)。これを10BASE-TのLANスイッチのポートに接続すると、問題なく通信できる。規格上保証された最大伝送距離の100mまでなら、ケーブルを伸ばしても大丈夫だ。一方、100BASE-TX(最大伝送速度は100Mビット/秒)のポートにつないだ

場合、ケーブルの距離が数mなら問題ない。ところが、ケーブルの距離を延ばすと、通信が不安定になる。

一般に信号がうまく伝わらない原因としては「長距離を伝送するうちに信号が弱まる」ことや、「ケーブルに様々な雑音(ノイズ)が混入する」ことが考

えられる。ノイズの影響は信号を高速に伝えるほど、顕著に現れる。カテゴリ3のケーブルで長距離を伝送する場合、100Mビット/秒まで高速化すると、距離による信号の減衰とノイズの悪影響などによって信号が正常に届かないと推測できる。



020

NFCとFeliCaはどこが違うの?

FeliCaはNFCの実装形態の一つだ。NFCは13.56MHz帯の周波数を使った無線通信規格のことである。NFC対応の機器同士を10cm程度まで近づけると、双方向に通信することが可能だ。データ伝送速度は106k、212k、424k、848kビット/秒。近距離、低速でデータをやり取りするので、通信を傍受されにくいなどの特徴がある。

NFCの規格はISO/IECで標準化

されている。2003年には「ISO/IEC 18092」、2005年にはその拡張仕様「ISO/IEC 21481」として、無線通信に使うプロトコル部分が規格化された。

プロトコル部分には標準規格があるものの、他の部分の実装はベンダーごとに異なり互換性がない。例えばFeliCaはプロトコル部分にISO/IEC 18092を採用し、ICチップ、ファイルシステム、データの暗号化処理などはソニー

が独自に実装したものだ。

現在、「NFCフォーラム」という業界団体が、無線通信のプロトコル以外の実装も含めて標準化を目指している。データの暗号化処理などセキュリティ部分に関しては決まっていないなど、現時点では課題が多い。NFCフォーラムでは技術的な標準化活動に加え、NFC対応機器間の通信の認定プログラムの作成なども進めている。

021

IPv4グローバルアドレスは、もう完全になくなっちゃった?

日本を含むアジア太平洋地域のRIRであるAPNICならびに、日本のNIRのJPNICが持つIPv4グローバルアドレスの在庫は事実上枯渇した。一方、プロバイダーやデータセンターには過去にAPNICやJPNICが割り振ったIPv4アドレスの在庫が残るが、手持ちの分を使い切ったら終わりだ。

APNICやJPNICは、最後の「/8」ブロックを残すばかりの段階を「事実上の枯渇」と呼ぶ。最後の「/8」は(1)「新規の事業者」「IPv6移行の目的」で分配する、(2)基準を満たせば1組織

に1回、最大「/22」ブロックを割り振るという特別な分配ポリシーで扱う。

プロバイダーやデータセンターは、上記の特別な分配ポリシーを満たさな

いと新規の割り振りを受けられない。そこで、「移転」制度を使って他の企業や組織からIPv4グローバルアドレスを購入するところも出てきている。

世界の五つのRIRのIPv4グローバルアドレス在庫

(インテックの「IPv4枯渇時計」より。2012年3月16日時点の数字)

RIRの名称	残りブロック数※	枯渇日(予測も含む)
AfriNIC	2.06	2014年10月29日
APNIC	0.94	2011年4月15日
ARIN	4.01	2013年7月27日
LACNIC	2.25	2014年1月28日
RIPE NCC	2.48	2012年8月8日

アジア太平洋地域の在庫は既に枯渇

※ 1ブロックは「/8」(1677万7216アドレス)

AfriNIC: African Network Information Centre
APNIC: Asia Pacific Network Information Centre
ARIN: American Registry for Internet Numbers

LACNIC: Latin American and Caribbean Internet Addresses Registry
RIPE NCC: Réseaux IP Européens Network Coordination Centre
RIR: Regional Internet Registry

022 Web掲示板に書かれた内容の著作権は誰にあるの？

掲示板への投稿内容が他者の著作権を侵害しているケースは論外だが、原則、著作権は投稿者にある。

気になるのは、そのサイトの利用規約に「投稿したコンテンツの著作権はサイト運営者に譲渡する」旨が記されているケースだ。日比谷パーク法律事務所^{かみやま ひろし}の上山 浩弁護士は、「規約に同意したうえで投稿していても、実際にすべての規約を読み、理解している利用者は少ない。利用者側に著しく不利な規約と考えられ、消費者契約法の下、著作権の完全な移転は認められにくい」と説明する。著しく不利というのは、権利を完全に移転するとすると、投稿者自身が投稿内容を再利用できなくなるからだ。

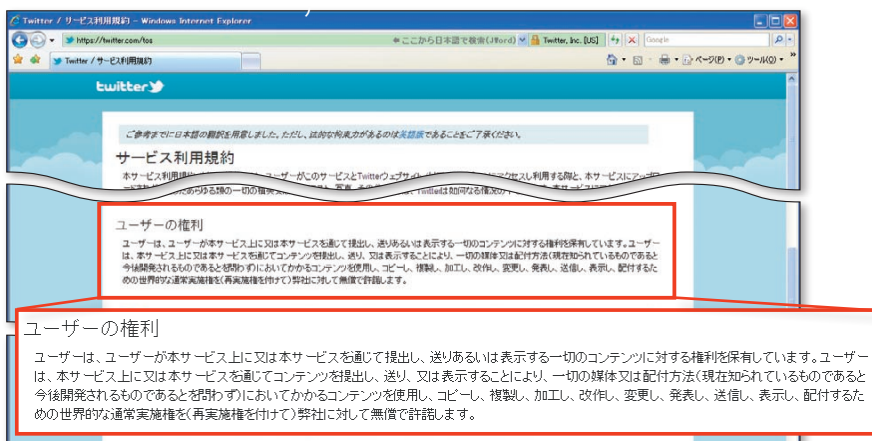
そこで現在は、投稿者も運営者側も自由に再利用できるような規約になっているサイトが多い。例えばTwitterの

場合、「ユーザーは、…一切のコンテンツに対する権利を保有しています」としたうえで、「コンテンツのコピーや複製、加工などの実施権をツイッター側に無償で許諾する」旨を規約に載せている(図)。

さらに、投稿内容をまとめて書籍などにする場合、再利用料を支払う

ケースが多い。もちろん名乗り出た人すべてに言い値を渡すわけではない。本人確認をし、一般的な印税などから妥当と考えられる金額を支払う。上山弁護士はサイト運営者に対し、「本人確認や支払い方法などの方針を事前に決め、差し止めや損害賠償のリスクを認識しておくべき」とアドバイスする。

Twitterにおけるサービス利用規約(<https://twitter.com/tos>)



023 パスワードはどのくらい長いと安全？

単純に考えれば、パスワードは長ければ長いほど安全となる。パスワードが長ければ組み合わせの数が増え、すべての組み合わせを試す総当たり攻撃(ブルートフォース攻撃)に対して強くなるからだ。ただし、パスワードが長くなると覚えておくのが難しいなど、運用が困難になる。

ジェービーサート JPCERTコーディネーションセンター(JPCERT/CC)早期警戒グループ情報セキュリティアナリスト マネージャー^{なかたに まさゆき}の中谷 昌幸氏によると、「単純に長さだけに注目するのではなく、文字の種類を増やすなど複雑なパターンにすることが重要だ」と指摘する。例えば、4けたの暗号でも、0~9の数字だけなら組み合わせは1万パターンだが、大文字と小文字のアルファベットを含めると約1500万パターンになる。

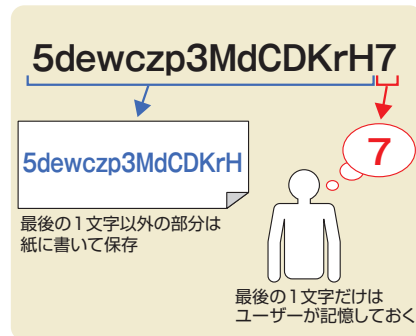
暗号化システムの種類によっても強度が変わるため、パスワードに必要な長さも変わってくる。例えば、暗号化^{ジップ}ZIPファイルのようにローカルに置いて自由に試せる場合、現在のパソコンならパスワードをかなり長くしてもあっという間に解読されてしまう。一方、決められた回数だけパスワード入力を誤るとロックがかかるシステムなら、総当たり攻撃ができないのでパスワードが短くても安全といえる。

ただ、オンラインバンキングのように重要なものについては、比較的長いパスワードで安全性を高めたい。しかし、長いパスワードは覚えにくいので、メモに残しておくことになる。この際、「ネット上での攻撃が盛んになった現在、データの形でパソコン上に置いておくよりも、むしろ紙に書いた方が安

全だ」と中谷氏は指摘する。

そうするとメモを紛失して誰かに見られることが心配になるが、そうした場合にも安全を確保できる工夫がある。「パスワードの最後の1文字だけはメモに残さずに、暗記しておく」(中谷氏)というもの。こうしておけば、もしメモを見られたとしても、その内容だけで暗号を解かれることはない。

長いパスワードを安全に運用する工夫の一例



024

ウイルスや攻撃手法の名前はどやうやって付ける?

ウイルスや攻撃手法の名前は、セキュリティソフトベンダーやOSベンダーなどが付ける。このため、同じウイルスでもベンダーごとに異なる名前が付けられることがある。例えば、2009年に猛威を振るった、不正なRPCリクエストを送り付けて感染を広げるウイルスを、シマンテックは「Downadup」、トレンドマイクロは「DOWNAD」、マイクロソフトは「Conficker」と名付けた。「ウイルスを調査したエンジニアが名前を付けることが多い」(トレンドマイクロ)という。そのためか、ウイルスの挙動やプログラムコードの特徴的な表記、ウイルスが誘導する攻撃サーバーのドメイン名などが付きやすい。ただし、「同一のウイルスに対して複数の名前が存在するとユーザーが混乱するため、他社が名付けたウイルス名に変更することがある」

ウイルスのファミリー名(この場合は「DOWNAD」)や分類名、感染対象のOS名などが入るのが一般的

亜種を区別するためのアルファベット。A、B から始まり、Z の後、AA、AB となる

WORM_DOWNAD.AD

ワーム

ダウンロード

※トレンドマイクロの場合

025

自炊代行は違法なの?

「自炊」とは、購入した書籍をスキャナーで電子化すること。著作権法では、「個人的に、家庭内やそれに準じる限られた範囲内で使用する」ためであれば、「著作物の複製」は自らが行う限り基本的に認められている。そのため、自炊そのものは違法ではない。

問題は、業者が代行するケースだ。利用者が書籍を送付すると、裁断からスキャン、電子化までを行うサービスである。電子化した後の書籍は、利用者に返送したり業者が処分したりする。代行業者は2011年に急増し、その年末には、7人の小説家や漫画家が特定の代行業者を相手に行為の差し止めを求める訴訟を起こした。内田・鯨島法律事務所の伊藤 雅浩弁護士は「まだ判決が出ていないために個人的な意見になるが」と前置きしたうえで、「業者側は『実質的にはユーザーの私的目的利用である』と主張すると考えられるが、現行法の枠組みでは認められないのではないかと予想する。

026

携帯電話を海外に持ち出しても、日本と同じ番号で着信できるのはなぜ?

日本の携帯電話機を海外に持っていくと、渡航先によってはそのまま着信できる。これは、国際ローミングサービスのおかげだ。日本の携帯電話事業者がローミング契約を結んだ現地の事業者の回線と国際回線を使ってつなぐ。海外に行くと、まず現地の事業者がIMSI^{イムジイ}と呼ばれる識別番号を使って端末を認識する。そして、現地の事業者は日本の事業者に認証情報を送り、電話がかかってきたら日本側で認証して着信させる。IMSIはSIMカードに記録された唯一の番号である。

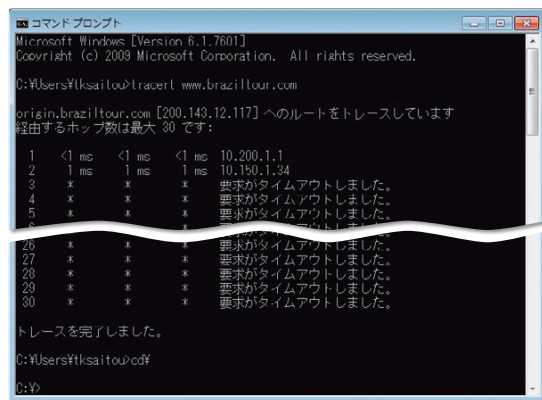
027

地球の裏側に設置されたWebサーバーにアクセスするとき、経路はどうやって決まるの?

インターネットは、各プロバイダーのネットワークの相互接続で成り立つ。プロバイダー内の経路は各プロバイダーのポリシーで決まり、次にどのプロバイダーに転送されるかはプロバイダー間の取り決めによる。

では地球の裏側、例えばブラジルに設置されたWebサーバーにアクセスする場合、どんな経路を通るのか。NTTコミュニケーションズのOCNサービスでは、2012年3月時点で「日本→米国→ブラジル」という経路になることが多いという。

なお経路の確認は、tracert^{トレースルート}コマンドを使って経路上にあるルーターのIPアドレスを調べる方法が一般的。ただ、tracertの通信が遮断されていることが多く、実際はほとんど確認できない。



028

マルウェアって いくつある？

マルウェアの数は、ウイルス対策ソフトウェアやセキュリティ関連サービスプロバイダーなどが公開している。ただ、ベンダーによって数え方が違うので、業界統一の答えはない。例えば、ドイツのセキュリティベンダー、AV-TEST^{エイブイテスト}によれば、2011年に確認したマルウェアは1770万9339個。2010年が1756万9794個だったので登場数はほぼ横ばいだ。一方、米シマンテックは2010年に確認したマルウェアは2億8600万個とAV-TESTと1けた違う。

数え方に違いが出るのは、グレーウェアと呼ばれるマルウェアなのかそうでないのか判定しにくいものの存在と、亜種の判断が各ベンダーで変わるからだ。亜種とは、マルウェアのプログラムコードを一部変更したり、手法だけをまねて作り直したりしたもの。ウイルス対策ソフトの検出を逃れたり、より大きな被害を与えたりするために改変される。

029

セキュリティ被害に 遭ったら、どこかに届 けないといけない？

ウイルス感染や不正アクセスといったセキュリティ被害に遭ったとき、被害者はどこかに届けなければいけないのか。セキュリティ被害の報告を受け付ける機関は、情報処理推進機構（IPA）、JPCERT/CC^{ジェービーサート シーシー}、都道府県警察本部のサイバー犯罪相談窓口がある。ただし、これらへの報告義務はない。

これらの窓口で報告をしてメリットがないわけではない。例えばIPAやJPCERT/CCでは、被害の受け付けだけでなく問題の切り分けや対処の助言などを行ってくれる。JPCERT/CCでは、フィッシングサイトや攻撃サーバーなどの存在がわかれば、そのサーバーをシャットダウンするよう、プロバイダーなどに掛け合ってくれることがある。ただし、「被害が外部に漏れることを嫌う企業が多く、実際届けているところは少ない」（セキュリティベンダー関係者）というのが現状だ。

030

いまさらだけどNGNって何？

NGN（次世代ネットワーク）は一般に、インターネット接続と電話、固定アクセスと無線アクセスといった様々なサービスを統合する通信事業者のIPネットワークを指す。日本国内では、主にNTTのNGNを指すことが多い。

NTTのNGNは、加入電話と同等の品質を持つIP電話サービス「ひかり電話」と、プロバイダー向けの光アクセス接続サービスの両方を統一的に提供する。以前はひかり電話とアクセス接続サービスは別のIPネットワークで提供されてきた。ひかり電話には高い信頼性とQoS^{QoS}機能が求められ、一方ベストエフォート型のアクセス接続は大容量・低コストが求められるからだ。

これらの異なる性質のサービスを一つのネットワークに統合するため、NGNでは両方の機能を一つのネットワークに組み込んだ。具体的には、コアネットワークはIPパケットの転送に特化させ、境界部に置いたサービスエッジで帯域確保や輻輳制御を実施する。

現在、NGN上で提供されているサービスとしては、エンドユーザー向けの「フレッツ 光ネクスト」「フレッツ・VPNゲート」「フレッツ・VPNワイド」「データコネクト」がある。また事業者向けサービスとしては、プロバイダー向けのIPv4/IPv6^{IPv6}接続サービスやコンテンツ配信サービスの「フレッツ・キャスト」などがある。