ネットワークへのウイルス感染対策

感染対策の基礎知識

#300

ティム・バーナーズ・リー

【インターネットと LAN Local Area Network】インターネットも LAN も TCP/IP という規約に沿って作られたパケット（前後をヘッダーという特別の数字で囲まれている一連のデータ列）を交換して通信を行う。 TCP/IP（Transmission Control Protocol over Internet Protocol）は英国のティム・バーナーズ・リーがスイスの **CERN**（**C**onseil **E**uropeen pour **R**echerche **N**ucleaire、欧州原子核研究機構）在籍中に構想を得た。 Web ページを写真や図とともに記述するための HTML（Hypertext Markup Language）や PC のネット上のアドレスを示す数字列、URL（uniform resource locater、通信中は PC のネットワーク・インターフェース・カード NIC にルータから 192.168.0.1 のような番号（DHCP というプログラムで自動的に割り振られる）も彼の考案による。 インターネットはすべての参加者と平等に通信ができるように工夫されているので、セキュリティーや秘密保持という概念は存在しなかった。初期のインターネット使用者は自身がプログラマで自分が便利に使いたい機能を提案し、皆の意見を RFC（Request for Comment）というタグをつけて公募した。 このため internet の規格書は RFC xxx 番とよばれる。 インターネットの世界は全て**善意の科学者、研究者が実験データを高速に安価に交換して、科学技術の発展に寄与する**ことだけが目的のシステムで、国境などの束縛や政府の管理から全く自由な存在であるのがインターネットの理想であった。 日本では junet（東大を中心に都内の数大学間で通信網を形成した）がはじまりで modem で電話回線を利用した。 これに対し銀行や鉄道など企業が乗車券の予約や口座の引き落としのための**【商用通信】**は秘密の保持と他者へのリークを防ぐ必要があり、「全銀協端末」やみどりの窓口の「マルス端末」は専用回線と専用の手順（protocol）を使用するので維持費用は莫大なものになる。 インターネットでは宛先 url を探してまずは隣に接続されている PC の中を探し、なければ別の PC へ移動するという形で通信経路を確立するので、最初は能率が悪いが、一度通信経路が確立すれば経路図を自分の PC の中に持ち二度目からは高速に接続できる。 Amazon などネットショップが成功すると安いインターネットを商用に利用する要望が強くなり、インターネット上で**【仮想プライベートネットワーク（VPN virtual private network）】**手順が使われるようになった。 厚労省や国立精神・神経医療研究センターが中心の 630 調査ネットワーク（正式名「精神福祉資料」、6 月 30 日に行われていた）も VPN で無線 LAN は使用せず、有線でルータと接続する。 ルータはハードウエアで **ipsec 手順の暗号化**を行いインターネット上に送出する。 仮想プライベートネットワークの相手方も ipsec 手順で暗号を復号できるルータを使用してデータベースを構築する。 暗号が破られなければネット上の他人により解読されることはないので仮想的にプライベートなネットワークが構築できる。 一方、通常のインターネットでは誰とでも通信ができるように手順やコードが共通化してあり、無線 LAN のみ暗号を使用する。 通常のネットワークで使用した USB メモリ、プリンタ、PC などの機器を VPN（仮想プライベートネットワーク）に接続した PC につなぐと VPN の隔離が破れて VPN の内容が通常のインターネットに流出する。 このため VPN に接続してある機器（医局の 2 台の PC）の USB ポートに通常のネットで使用した機器をつないではいけない。**VPN に接続するプリンタは専用プリンタとし**、VPN 外の機器と接続しない。 **USB 接続時にデバイスドライバーが自動的にプリンタからロードされるので、ウイルスも一緒に VPN のネットワーク内に持ち込まれる。 VPN 専用プリンタ**も他のインターネットにつながる PC に接続されたことのあるものは決して VPN と接続してはいけない。 当院では 630 調査用の PC にプリンタをつないで印刷するのを見かけるので、厚労省の 630 調査のネットワークは当院のプリンタを介して通常のネットワークとつながっており、ここで隔離が破綻している。

*1