ネットワークへのウイルス感染対策
（仮想プライベートネットワーク VPN）

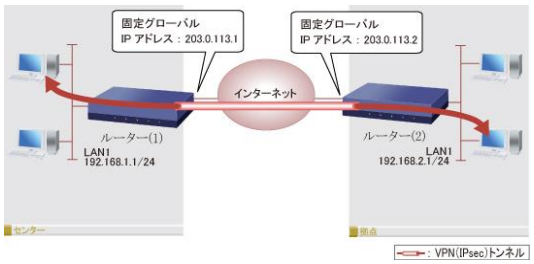

ティム・バーナーズ・リー

https://l-hospitalier.github.io 2018.12

感染対策の基礎知識

#168

【インターネットと LAN, Local Area Network】インターネットも LAN も TCP/IP 規格のパケット（先頭にヘッダー・コードを持つデータ列）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（欧州原子核研究機構）在籍中に構想を得た。 Web を写真や図とともに記述するための HTML（Hyper-Text Markup Language）や PC のネット内の位置（サイト）を示す url（uniform resource locater、192.168.0.1 のような数字列 = IP アドレス）も彼の考案。 IP アドレスは固定、あるいはルータから DHCP Dynamic Host Configuration Protocol プログラムで PC のネットワーク・インターフェース・カード（NIC）に自動的に割り振られる*1（時間リース）。 インターネットは全ての参加者が平等に通信することが目的なのでセキュリティや秘密保持という考え方は存在しなかった。 初期のインターネット参加者は全員がプログラマで便利な自分が使いたい機能を提案、皆の意見を RFC（Request for Comment）*2 というタグをつけて公募したので internet 規格は RFC xxx として規格化。 インターネットは全て善意の科学者、研究者が実験データや理論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を目的とするシステムで国境の束縛や政府の管理から自由な存在であることがインターネットの理想であった。 日本では JUNET（慶応、東工大、東大を中心に都内の大学間で通信網を形成）がはじまりで modem で電話回線を利用した。これに対し銀行、鉄道や航空などの企業が乗車券の予約発券や口座の引き落としのために使う【商用通信】では秘密の保持と他者からの改変を防ぐ必要があり全銀協の ATM や JR みどりの窓口のマルス端末は専用の回線と手順（protocol）を使用し維持保守費用は莫大。 インターネットでは宛先 url を探して、まずは近隣の PC のキャッシュを探索、なければゲートウエイから出て別の PC を探索する方式で通信経路を確立するのに最初は効率が悪いが一度経路が確立すれば経路のキャッシュを自分の PC に持ち、高速に接続できる。 電話も Skype 等あるが普通は商用回線を維持。 Amazon などネットショップが成功すると廉価なインターネットの商用利用の要望が高まり、ネット上で【仮想プライベートネットワーク（VPN virtual private network）】が使用可能になった。 医療業界では臨床検査センター企業（BML）は患者の検査データをハードウエアの ipsec 手順の暗号化ルーター（YAMAHA 製が多い）を使ってインターネットに送出する。 契約病院の検査室では受信した暗号をルータで復号して専用の PC と専用プリンタでデータをプリントアウト。 暗号が破られなければネット上の他人に解読されることはないので仮想的にプライベート（私用）ネットワークが構成できる。 FAX で検査データを送信する場合は暗号化しないので電話番号を間違えると検査データは誰でも読める形で誤配（家には黒猫ヤマトの間違い FAX が来る）。 インターネットは誰とでも通信ができるように手順やコードが共通（無線 LAN では WPA2 暗号を使う）なので、通常のネットで使用した USB メモリ、プリンタ、PC などを VPN に接続した PC の平文（ひらぶん）が流れる経路（暗号化以前、復号以後の箇所）に接続すると VPN の隔離が破れてウイルスが混入する危険がある。 VPN に接続した PC の USB ポートには何も接続せず隔離が安全。 不用意に USB ポートに接続するとデバイスドライバが自動的にロードされるので、ウイルスも一緒に VPN ネットワーク内に持ち込むことがある（USB メモリは小さなコンピュータ）。 逆に通常のインターネットに接続される機器はソフトウエアのセキュリティ・ホールの改修のため常にネット上の更新ソフトウエアのインストールを続ける必要がある。 ランサムウエアに対してはシステムとデータのバックアップは必須。ファイアウォール、ディフェンダーも設定確認。



*1 外部からアクセスするサイトは固定 IP アドレス。 *2 インターネットの名前の管理や運営（ルートサーバー）は ICANN, Internet Corporation for Assigned Names & Numbers（非営利団体）が、技術面は IETF, Internet Engineering Task Force が RFC で行う。 IETF 総会 3 回のうち 1 回は世界各国で開かれ誰でも参加 OK。 採決は議長の指示で賛成は鼻歌（ハミング）を歌うラフ・コンセンサスとする（反対は静粛）。 原則的にインターネットに禁止事項はない。