ネットワークの管理コマンド

感染対策の基礎知識

#169

https://**l-hospitalier.github.io**　＜－　まずここにアクセス！　**2018.12**

【shell と kernel】シェルはネット管理人（Administrator、略は Admin）が使うユーザー･インターフェース。**カーネル**が通信の割り込みやストレージ､メモリを管理。UNIX では Bourne Shell（B-shell）や C-Shell、bash を使う。 Windows ではアクセサリ→コマンドプロンプト（Win7）や PowerShell（Win10）。PowerShell を起動して **PS:¥Users¥xxx>**_プロンプトの後にコマンド入力。**【>ipconfig/all】**で＜**イーサネットアダプタ**＞以下に ①ホスト名（コンピュータ名）②物理アドレス（**MAC** アドレス､**M**edia **A**ccess **C**ontrol Address）③**DHCP** 有効（固定 IP アドレスか DHCP で IP アドレスをリースされているか） ④IPV4 アドレス（192.168.xxx.xxx）[*1]、IPV6 アドレス ⑤サブネットマスク。 クラス C のマスクは 255.255.255.0 で 254 のアドレスを持つネット空間。 IP アドレスとサブネットマスクのビット and 演算の結果がネットワーク名、最後のオクテットがサイト番号 ⑤デフォルト・ゲートウエイ（ネット内に目的地がない時の出口アドレス、通常はルータ（192.168.0.1）。無線 LAN があれば＜Wireless Lan Adapter＞以下にも同様の出力。**【 >ping IP アドレス】**潜水艦の超音波ビーコンと同じで周辺の PC を検索。 >ping 127.0.0.1（=localhost）は自分自身のチェックでサーバー（この場合はローカルホスト）からの応答。時間（ms）､パケット損失。**TTL**（**T**ime **T**o **L**ive、パケット生存時間）が示される。 TTL はルータを通過すると 1 減る。 TTL が設定されていないとゾンビ･パケットがネット内を走り続け､ネット･トラフィックは減少せず、ネットワークは飽和してやがてダウンする。**【 >command】**コマンドのリスト。**【>netstat】**TCP、UDP のプロトコル別。 ローカル IP アドレスと外部 IP アドレスの対応と接続状態のリスト。**【>arp- a】**address **r**esolution **p**rogram、IP アドレスと MAC アドレスの対応テーブルと静的／動的表示。 通常 arp パケットが自動的に対応を動的に割り振るが arp 非対応の NIC では手動で設定（静的）。**【>nslookup www.ocn.ne.jp】**でサイトの IP アドレスを DNS サーバーに問い合わせて知らせる（正引き）。>nslookup IP アドレスは url の名前を返す（逆引き）。**【その他のコマンド】** >dir、cd、su（super user）その他シェルコマンドは Win でも Linux でも使用可。 Win の PowerShell で FTP は使用できるが telnet は Security のため別途サービスとして起動しないと使用できない。コンピュータの創生期にはコンソールとメインフレームは RS-232c 非同期シリアル通信を介した telnet と FTP で操作した。 **telnet と FTP**（**F**ile **T**ransfer **P**rotocol）はコンピュータ操作の基本。 現在の PC のイーサネット上では telnet は IP アドレス：ポート 23 に接続。 telnet と FTP を接続すれば「PC を乗っ取る」と言うより「自分のコンピュータ」。 well-known port（0~1023）のポート 23 が開いていれば外部から操作できる。 今はポート 22 の scp 公開鍵暗号手順を使ってアクセス。**【フリーソフト】**ネット上では telnet（平文）に代わり SSH 暗号化ターミナル・ソフト（RLogin, Putty, TeraTerm）を使用。 FTP（FTPS、SFTP）は WinSCP や FileZilla。**【注意事項】**Win の MSG や net send コマンドはネット管理のためユーザーに直接連絡するコマンド。緊急時以外にこれらを使うとスクリーンに突然メッセージが現れるので乗っ取られたと思うユーザーがいるので注意。 RLogin のサブコマンドの port-scan を使って開いているポートを検索するのは悪質ハッキングとみなされる。 以下はネット・コマンドのリスト **arp（ARP テーブル表示）、ifconfig/ ipconfig（IP 構成表示）、hostname（ホスト名表示）、nbtstat（NBT ステータス表示）、netstat（ネットワーク･ステータス表示）、nslookup（DNS 問いあわせ）、ping（疎通確認）、route（ルーティング･テーブル保守）、traceroute（通過経路確認）**。外部インターネット接続時にローカル IP アドレス 192.168.1.xxx/24 が **IP マスカレード**（IP 仮面舞踏会）でどのグローバル IP アドレスに変換されているかは CMAN（サーバ／ネットワーク監視サービス）にアクセスすると教えてくれる。

[*1]192.168.x.0 は一般的にローカルネットワークで使うクラス C ネット空間の名称、192.168.x.255 はブロードキャスト・アドレス（ネット内全アドレスに同時送信）なのでクラス C 空間は 256-2=254 の IP アドレス空間。 サブネットマスク 255.255.255.0 は 192.168.x.x/24 と全く同じ意味で初めの 3 オクテット（24 bit）のマスクの意味。 アプリケーションは IP アドレス：ポート番号を指定して通信するので不使用ポートは閉じておく。 NetEnum によるネット内の IP スキャンとは ping コマンドでポート 7 の echo back を使用するので悪質行為ではない。