本資料について

本資料は下記著書を基にして作成されたものです。著書の内容の正確さは保障できないため、正確な知識を求める方は原本を参照して下さい

著書名：ネットワーク攻撃詳解
著者　：三輪信雄／新井　悠
出版社：ソフト・リサーチセンター

不正アクセスについて
(ネットワークの攻撃詳細)

渡邉研究室　　水野　邦彦

ポートスキャン

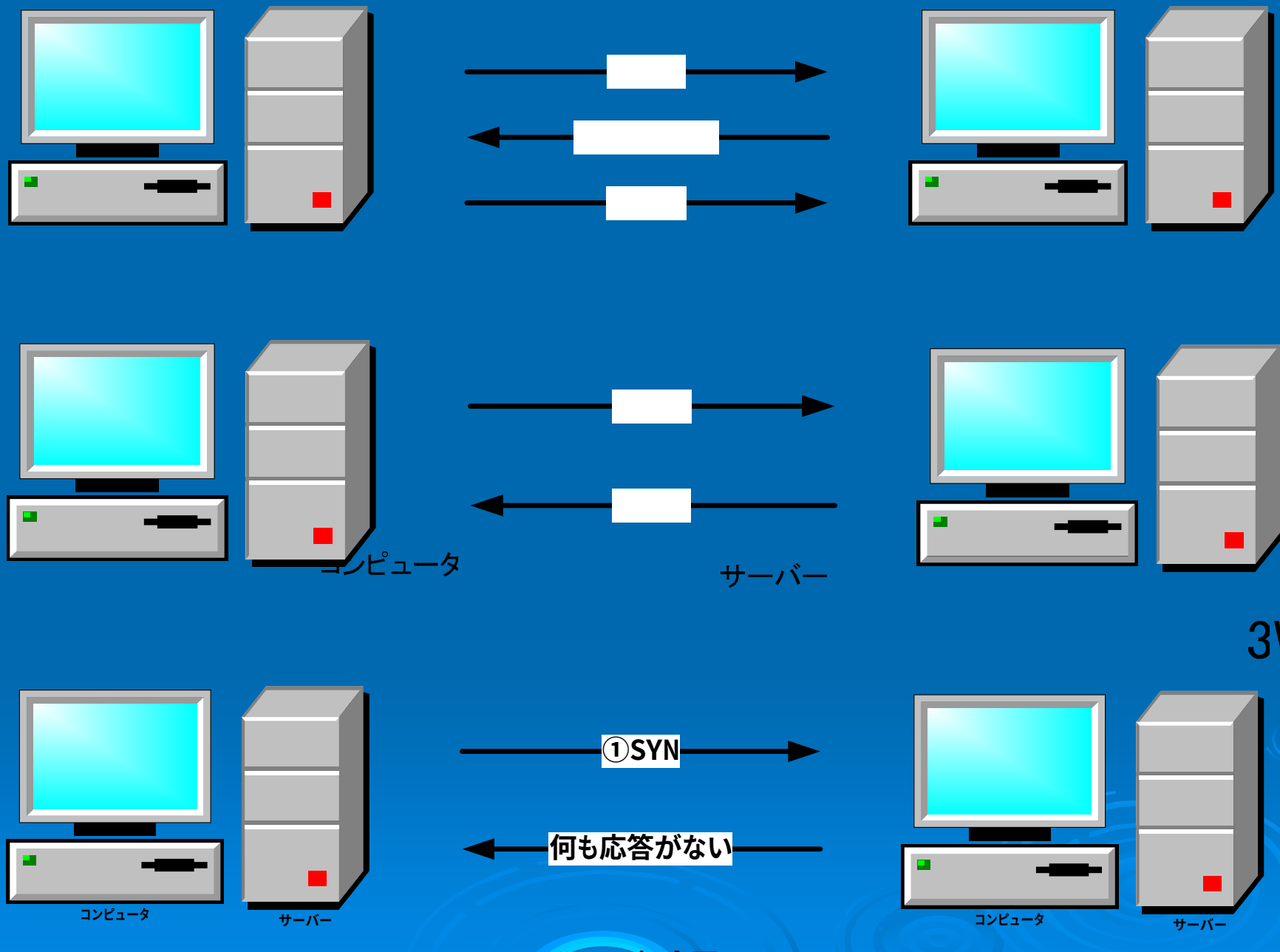
- Nmap
  - TCPスキャン
  - UDPスキャン
  - ステルススキャン
  - アイドルスキャン

nmap

- 数あるポートスキャナのうちでも非常にメジャーなものである。
- Fyordor氏によって開発されている、フリーのポートスキャナである。

TCPスキャン

- NmapによってTCPスキャンが実行される際には以下のような手順で行われている。
  - ①ターゲットホストのTCPポートにSYNフラグの付与されたパケットを送信
  - ②ターゲットホストからの応答を待つ
  - ③-1ACKフラグの付与されたパケットが戻ってくれば、そのポートは開いていると判断
  - ③-2RST/ACKフラグの付与されたパケットが戻ってきた場合はそのポートは閉じていると判断
  - ③-3SYNパケット送信後、何の音沙汰も無い場合は”filtered”を表示し、経路途中の協会ルータあるいはファイアーウォールによって通信が遮断されたということを伝える。

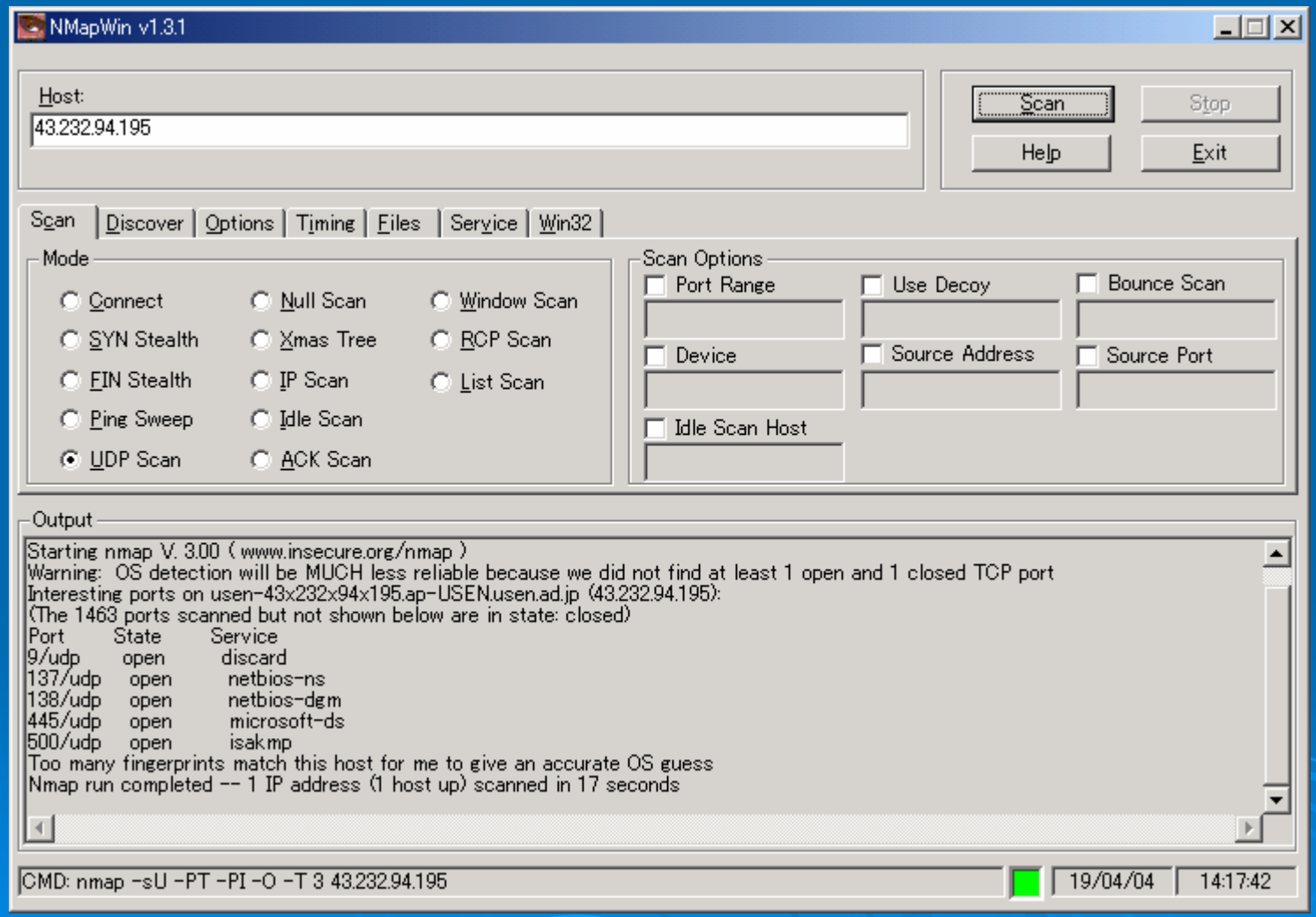


filtered概念図

UDPスキャン

- UDPスキャンを実行するには以下のようにする。
  - ①ターゲットホストのUDPポートにUDPパケットを送信
  - ②ターゲットホストからの反応を待つ
  - ③”ICMP　port　unreachable”というICMPメッセージが返ってきた場合は、そのポートは閉じていると判断。逆にそれ以外の値が返ってきた場合や、何も返ってこない場合などはそのポートが開いていると判断。

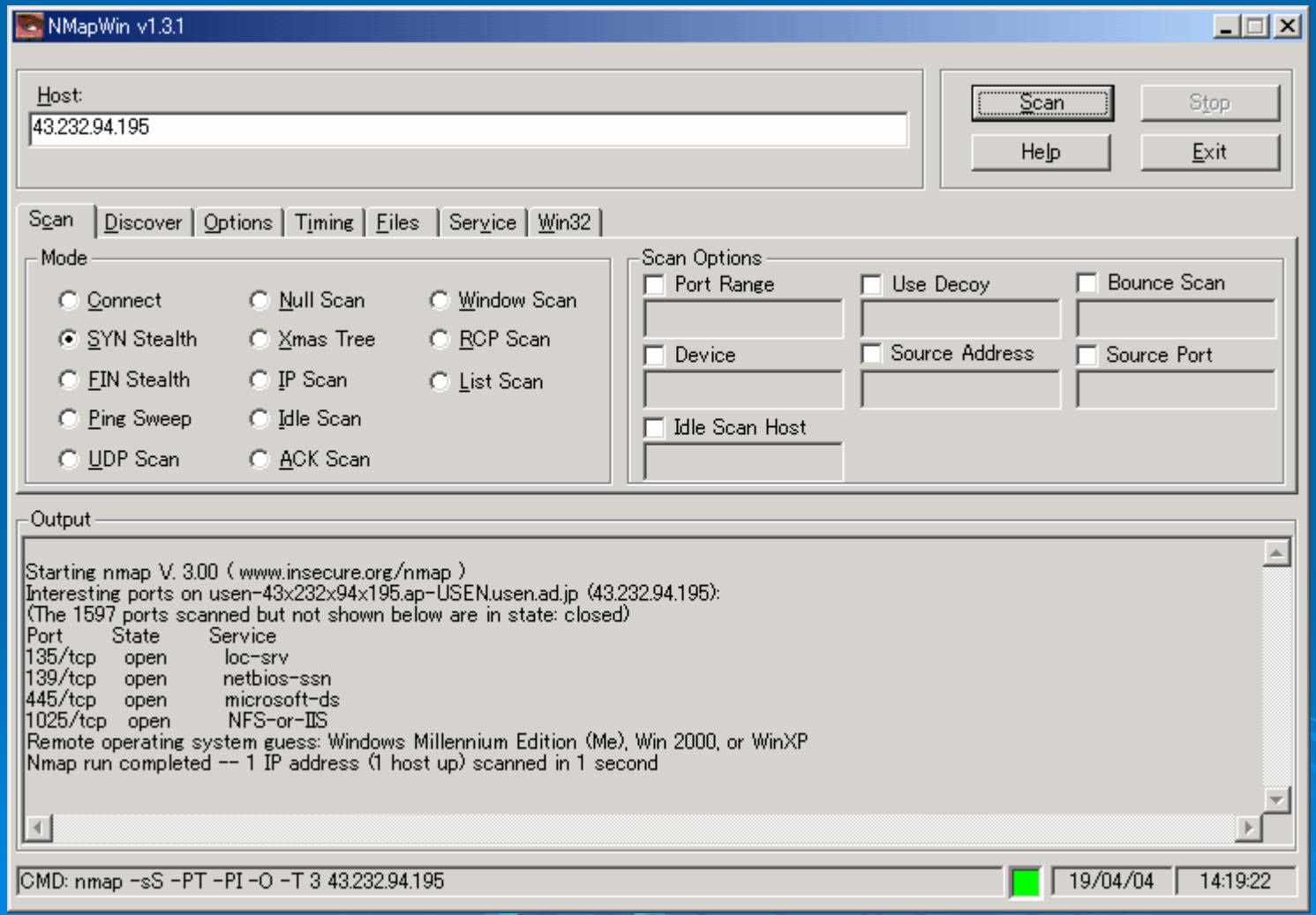
Nmapを使用してUDPスキャンを行った。



ステルススキャン

- このスキャンはTCPスリーハンドシェイクスキャンの最後のステップである。「接続元からのACK」を送信しないスキャン手法である。
- つまり、SYNを送信した後の戻り値がSYN/ACKであるかRST/ACKであるのかを分別することで、そのポートが開いているかどうかを確認することができる。

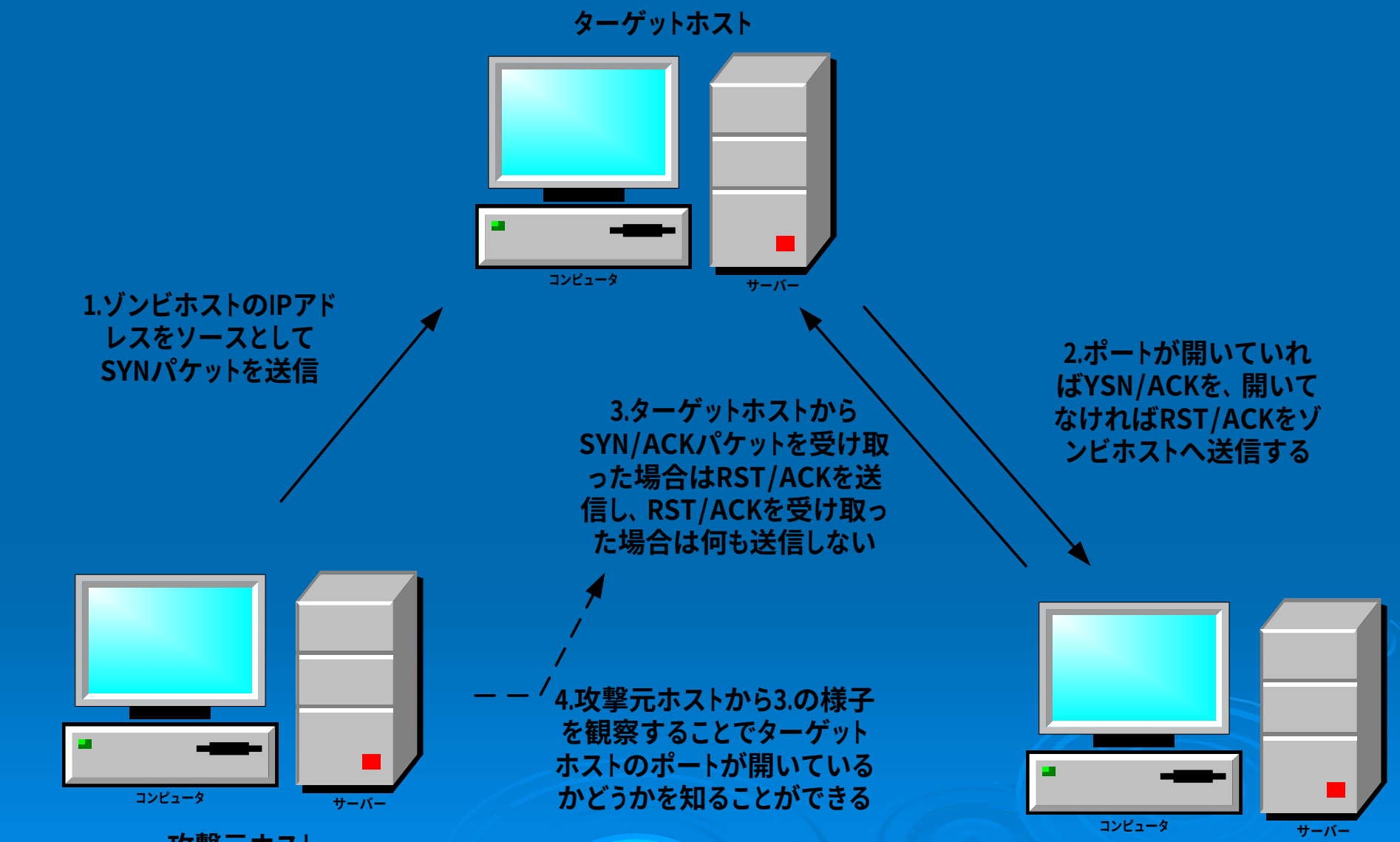
Nmapを使用してステルススキャンを行った



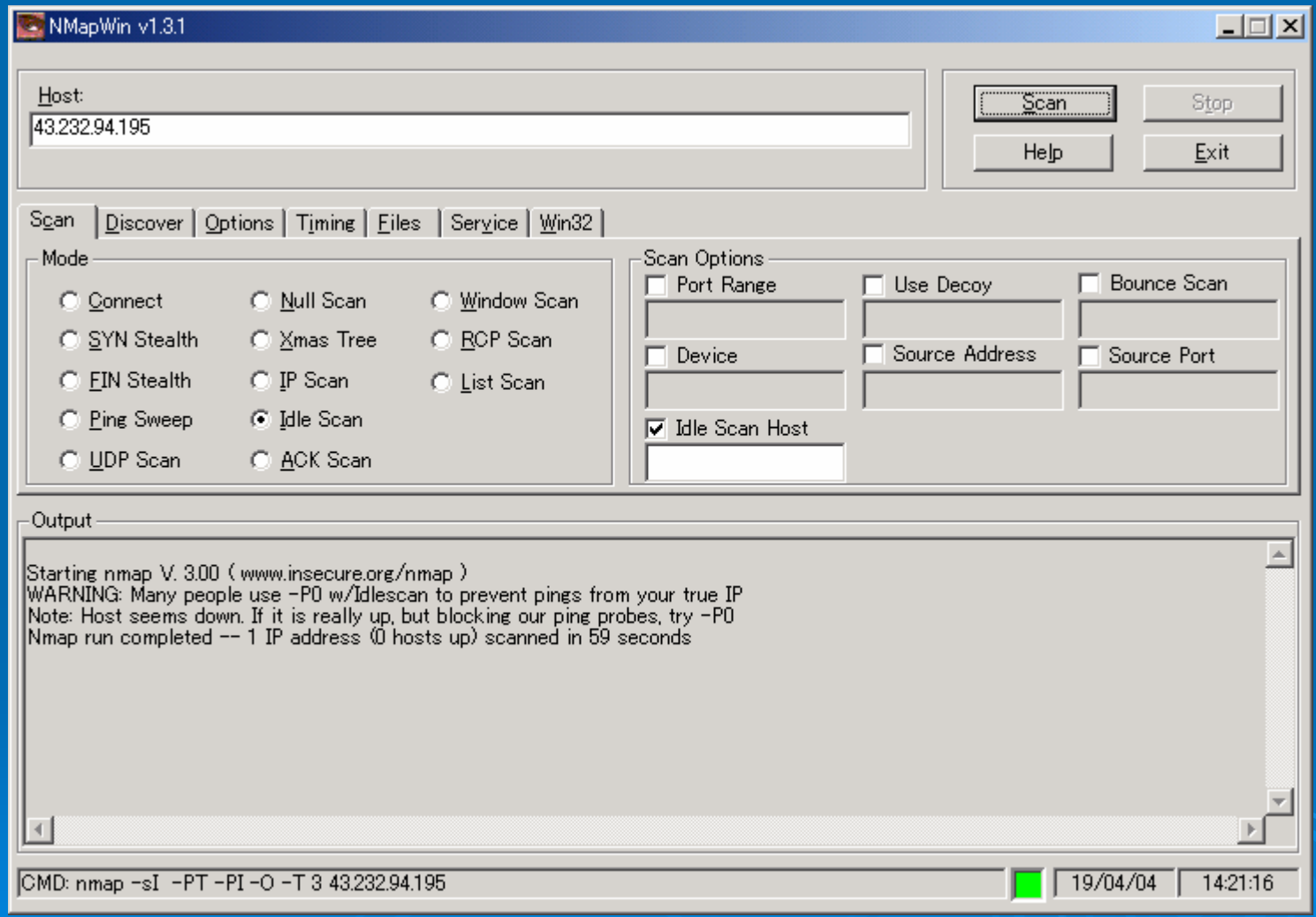
アイドルスキャン

- これはスキャン元のIPアドレスが全く記録されないというスキャンである。
- 簡単に説明すると、代理のスキャン用ホストを利用することで、ターゲットホストのポートの解放状況を判断することができる。

アイドルスキャンの概略図



Nmapを使用してアイドルスキャンを実行した結果



結果と感想

- スキャンの種類によって出てくる結果も少し違った結果がでることがわかった。
- まだまだ理解できてないので、どんどん理解を深めていきたいと思う。