7.10. nmap でポートの状態を確認する

nmap (Network Mapper)は、ネットワーク調査およびセキュリティ監査を行うためのツールです。

nmap コマンドではポート状態の一覧を表示できます。この一覧表には、ポート番号、プロトコル、サービス名、状態が記載されています。状態は、open、filtered、closed、または unfiltered のいずれかになります。

open

このポートでは、アプリケーションが TCP コネクションや UDP パケットをアクティブに受け入れています。多くの場合、ポートスキャンの第一の目的は、この種のポートを見つけることにあります。セキュリティを重視するなら、open ポートが攻撃者の通り道にならないようにする必要があります。ポリシーに合わせてファイアウォールで閉じたり防御したりするのが良いでしょう。また、Open ポートを見ると、ネットワーク上で利用可能なサービスが何かわかるので、セキュリティスキャン以外にもよく用いられます。

closed

closed(閉じた)ポートは、アクセス可能(Nmap のプローブパケットを受信したり応答したりする)ですが、そこで受信待機しているサービスやアプリケーションはありません。この種のポートは、ある IP アドレスでホストが稼動中であることを確認する場合(ホスト発見や ping)や、OS 検出の一環として役に立つ場合があります。closed ポートは到達可能なので、後にその一部が開放された場合は、スキャンの対象になる可能性があります。管理者はこの種のポートもファイアウォールでブロックすることを検討する場合もあります。そうなると、これらは次で述べる filtered(フィルタあり)状態として見えるようになります。

filtered

nmap は、このポートが開いているかどうかを判別できません。パケットフィルタによって、プローブがポートまで到達できないからです。このフィルタ処理は、ファイアウォール専用機器、ルータのルール、ホストベースのファイアウォールソフトなどで実行できます。これらのポートからは情報がほとんど得られないので、攻撃者の企てを阻むことになります。応答しないでプローブを破棄するだけのフィルタが多く使われるようになっています。この場合、nmap は、プローブが破棄されたのはフィルタリングではなくてネットワークの混雑のせいと見なして、再試行を数回行わざるを得なくなるので、攻撃者からのスキャンの進行速度が格段に落ちます。

unfiltered

unfiltered 状態とは、ポートにはアクセス可能ですが、そのポートが開いているか閉じているかを nmap では判別できないことを意味します。ポートをこの状態に分類できるのは、ファイアウォールルールを解読するのに使われる ACK スキャンだけです。unfiltered ポートのスキャンをその他のスキャンタイプ、例えば Window スキャンなどで

行うと、ポートが開いているかどうかを決めるのに役立つ場合もあります。

open|filtered

nmap がポートをこの状態に分類するのは、対象のポートが開いているかフィルタ処理されているかを判別できない場合です。open ポートからの応答がないタイプのスキャンには、こうしたケースが発生します。また、応答がないということは、プローブやそれが引き出した応答をパケットフィルタが破棄したことを意味する場合もあります。そのため nmap は、対象のポートが open なのか filtered なのかを確実に見分けることができません。UDP、IP プロトコルなどのスキャンは、ポートをこの状態に分類します。

closed|filtered

この状態は、ポートが閉じているかフィルタ処理されているかを、nmap が判断できない場合に用いられます。

```
# nmap www.ipa.go.jp

Starting Nmap 5.51 ( http://nmap.org ) at 2013-01-23 19:04 JST
Nmap scan report for www.ipa.go.jp (202.122.139.39)
Host is up (0.022s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```