

平成 26 年 2 月 6 日

## インターネット観測結果等 (平成 25 年 11 月期)

- レンタルサーバ会社の保有する IP アドレスを発信元とする宛先ポート 135/TCP に対するアクセスが増加
- 中国を発信元とする宛先ポート 22/TCP に対するアクセスが増加

### 1 レンタルサーバ会社の保有する IP アドレスを発信元とする宛先ポート 135/TCP に対するアクセスが増加

今期は、米国<sup>1</sup>を発信元とする宛先ポート 135/TCP に対するアクセスが増加しました(図 1)。

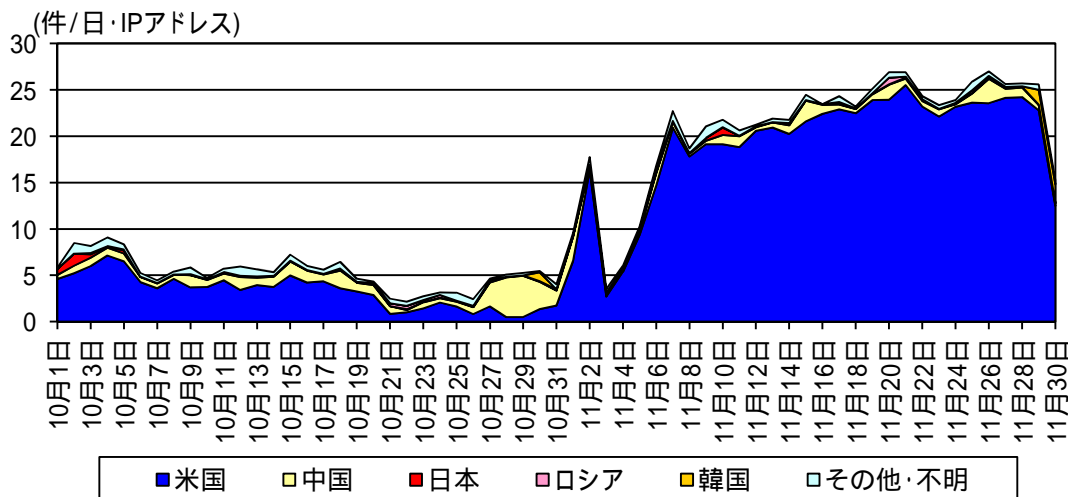


図 1 宛先ポート 135/TCP に対するアクセス件数の推移(10月～11月)

135/TCP は、ネットワークを経由したプログラム呼び出し(RPC)に使用されるポートであり、Microsoft Windows でも使用されています。インターネットに直接接続された Microsoft Windows が稼動するコンピュータを探索するスキャン行為であると考えられます。

同アクセスの9割以上は、発信元ポートが 4445/TCP に固定されており、同一のツールを使用したアクセスと考えられます。また、発信元 IP アドレスの多くは、米国に拠点を置くレンタルサーバ会社が保有している IP アドレスであることを確認しています。レンタルサーバ会社の提供するサーバからスキャン行為が行われている可能性があります。

135/TCP は、かつて Microsoft Windows の脆弱性を悪用した不正プログラムの感染活動にも使用されたポートであるため、再度、脆弱性を狙った攻撃の対象となることが懸念されます。

<sup>1</sup> 発信元国・地域については、当該国・地域に割り当てられた IP アドレスを指しています。

## 2 中国を発信元とする宛先ポート 22/TCP へのアクセスが増加

今期後半には、中国を発信元とする宛先ポート 22/TCP に対するアクセスが増加しました(図 2)。

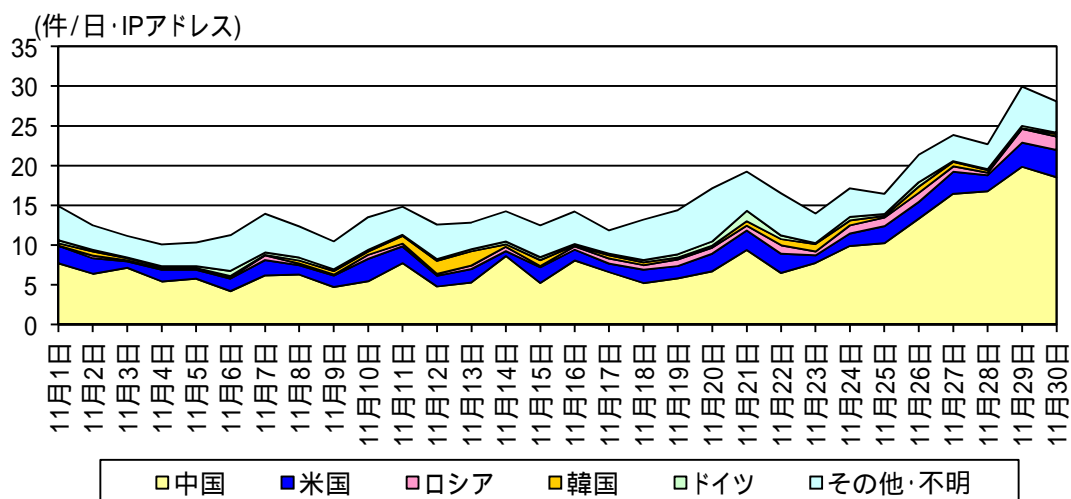


図 2 宛先ポート 22/TCP に対するアクセス件数の推移

22/TCP は、コマンドラインでの遠隔制御を可能にする SSH サービスで使用されるポートであり、SSH サービスが稼働しているコンピュータをはじめとしたインターネットに接続された機器の探索を行っていると考えられます。今期後半の中国からのアクセスは、発信元ポートが 6000/TCP に固定されているものが多く見られ、何らかのツールを使用したアクセスであると考えられます。