平成 26 年 8 月 27 日

インターネット観測結果等

(平成 26 年 7 月期)

- ビル管理システムに対する探索行為の継続
- 宛先ポート 23/TCP に対するアクセスが増加

1 ビル管理システムに対する探索行為の継続

ビル管理システムで使用される通信プロトコル用標準規格「BACnet」に定義された 47808/UDP へのアクセスを分析したところ、6 月下旬頃から検知した「ReadPropertyMultiple」のパケットを、今期も継続して観測しています（図1）。

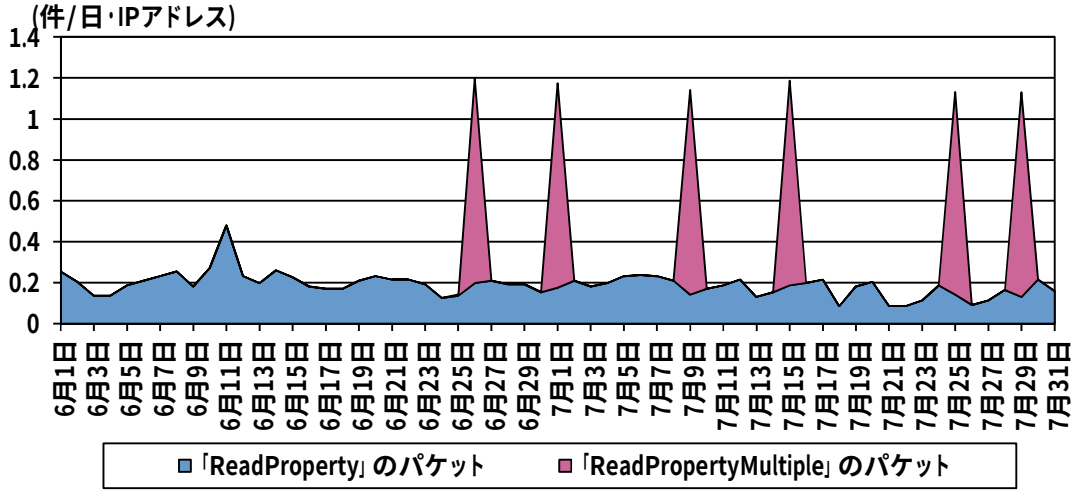

図1 宛先ポート 47808/UDP に対するアクセス件数の推移

警察庁では、ビル管理システムに対する探索行為の検知について、平成 26 年 4 月[i]、5 月[ii]及び 7 月[iii]に注意喚起を実施しているので参考として下さい。

[i] 「ビル管理システムに対する探索行為の検知について」（平成 26 年 4 月 4 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140404.pdf

[ii] 「ビル管理システムに対する探索行為の検知について（第 2 報）」（平成 26 年 5 月 8 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140508.pdf

[iii] 「ビル管理システムに対する探索行為の検知について（第 3 報）」（平成 26 年 7 月 6 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140706.pdf

2　宛先ポート 23/TCP に対するアクセスが増加

7月下旬頃から宛先ポート 23/TCP に対するアクセスが増加しています（図 2）。

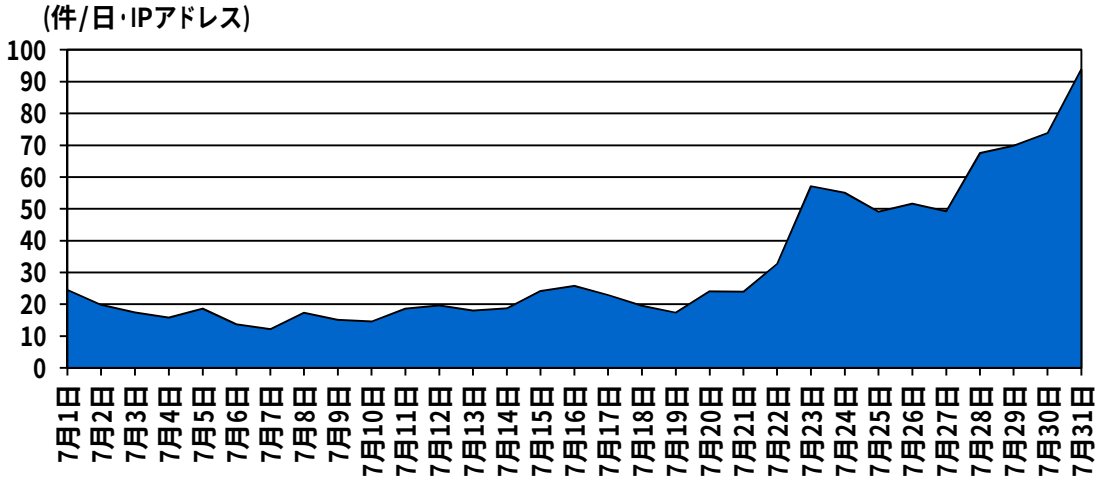

図2　宛先ポート 23/TCP に対するアクセス件数の推移

23/TCP は、Telnet に使用されるポートであり、遠隔でネットワーク機器等に接続する際に使用されるものです。このポートに対するアクセスの発信元 IP アドレスを調査したところ、2月頃に確認されたウェブカメラのログイン画面が表示されることを確認したほか、ルータのログイン画面（複数種類あり）が表示されることを確認しました。ことから、このポートに対するアクセスは、ネットワーク接続機器を踏み台にしたスキャン行為が行われている可能性が考えられます。