平成 26 年 5 月 2 日

インターネット観測結果等
(平成 26 年3月期)

● 3月中旬以降、ビル管理システムの基幹ネットワークに使用されている BACnet で使用されるポートに対する探索行為と思われるパケットの検知

1 宛先ポート 47808/UDP に対するアクセスの検知

3月中旬以降、宛先ポート 47808/UDP に対するアクセスを検知しました（図1）。

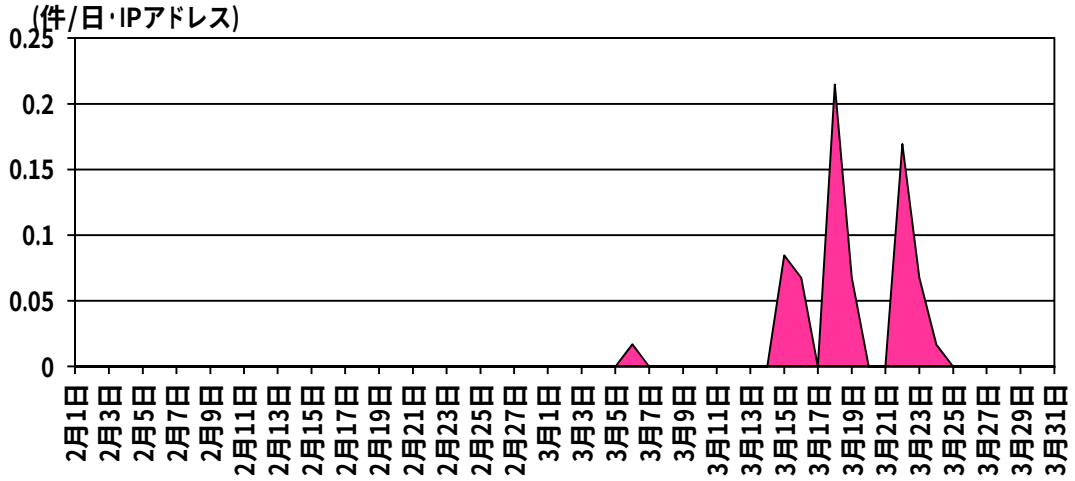

図1 宛先ポート 47808/UDP に対するアクセス件数の推移
（H26.2.1～H26.3.31）

47808/UDP は、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」で定義されているポートであり、このアクセスは、BACnet に基づいて構成されたシステム（BACnet システム）を探索している可能性があります。同アクセスを分析したところ、BACnet システムに接続された機器の情報を確認する「Read-Property」のパケットであり、BACnet システムの探索行為であると考えられます。

平成 26 年4月に注意喚起[1]を実施したので、対策等については、そちらを参考にして下さい。

2 宛先ポート 5000/TCP に対するアクセスが継続

2月中旬から宛先ポート5000/TCP に対するアクセスが増加しており、3月も継続して大量のアクセスを観測しました（図2）。

5000/TCP は、Synology 社製の NAS のウェブ管理画面に使用されているポートであり、脆弱性

[1] ビル管理システムに対する探索行為の検知について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140404.pdf

を持つ同製品を狙った攻撃活動であると考えられます。

平成26年3月に注意喚起[2]を実施したので、対策等については、そちらを参考にして下さい。

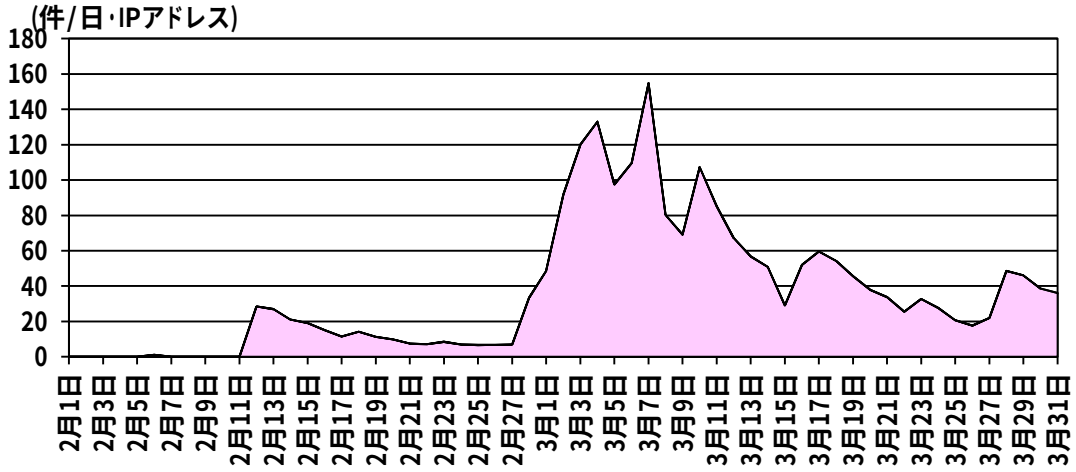

図2 宛先ポート5000/TCPに対するアクセス件数の推移（H26.2.1～3.31）

3 宛先ポート8088/TCPに対するアクセスが増加

2月下旬から宛先ポート8088/TCPに対するアクセスが増加し、3月も継続して大量のアクセスを観測しました（図3）。

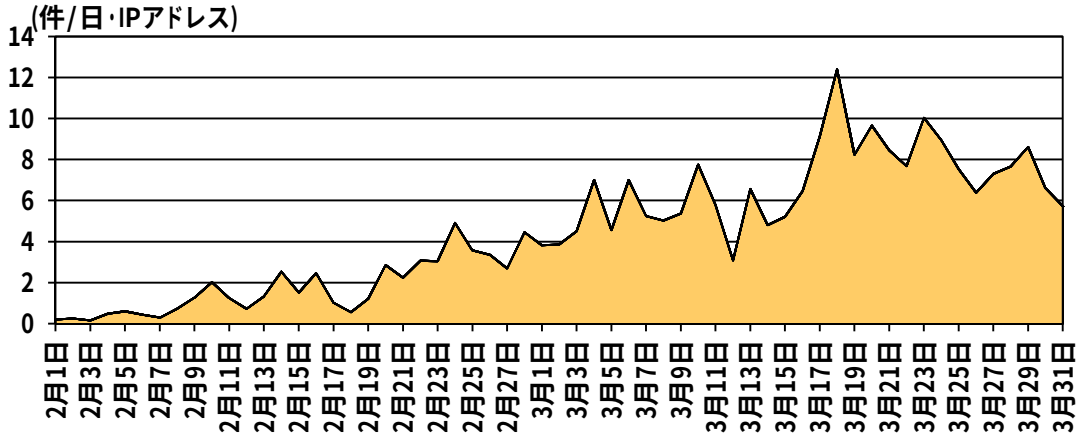

図3　宛先ポート8088/TCPに対するアクセス件数の推移（H26.2.1～3.31）

同アクセスを分析した結果、多くのアクセスはHTTPのGETリクエストであることが判明しました。プロキシサーバの中には8088/TCPのポートを使用しているものもあり、このポートに対するHTTPのアクセスは、公開されているプロキシサーバを探索している行為と考えられます。

---

[2] 脆弱性が存在するNASの探索と考えられる宛先ポート5000/TCPに対するアクセスの急増について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140305.pdf