平成 26 年 11 月 13 日

Topic

ビル等におけるエネルギー管理システムが踏み台となる危険性について

11 月 7 日以降、宛先ポート 23/TCP へのアクセスが急増しています。発信元の中には、ビル等におけるエネルギー管理システム（以下「EMS[i]」という。）の管理画面が確認されるものもあり、これらのシステムも踏み台となっている可能性があります。利用者についてはネットワーク機器も含めシステムが適切な設定になっているか確認することを推奨します。

1 23/TCP の増加

警察庁の定点観測システムでは、11 月 7 日以降、宛先ポート 23/TCP に対するアクセスの急増を観測しています（図 1）。23/TCP は、遠隔でコンピュータを操作するためのプロトコルである Telnet で使用されるものです。そのため、このアクセスは遠隔操作が可能なコンピュータを探索しているものと考えられます。

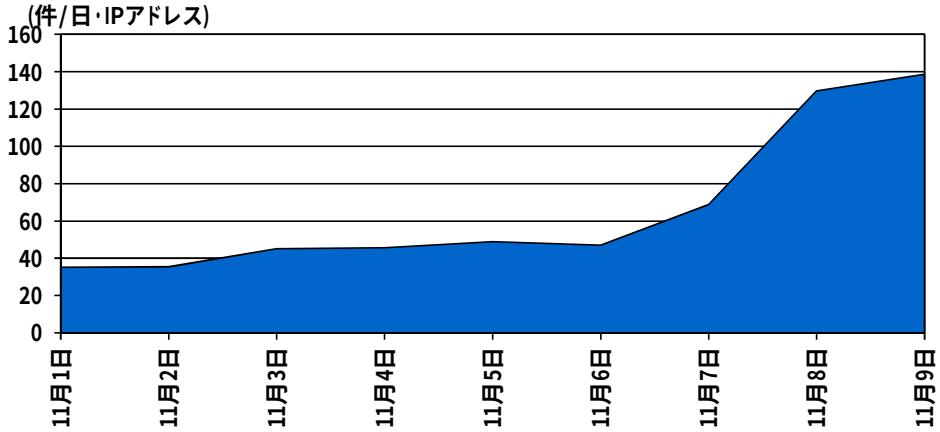

図 1 宛先ポート 23/TCP に対するアクセス件数の推移（11 月 1 日～11 月 9 日）

2 発信元の確認

宛先ポート 23/TCP に対するアクセスの発信元の確認をしたところ、これまでと同様に Web カメラ記録装置やルータ等のネットワーク機器のログイン画面が散見されました[ii]。また、発信元が日本のものに着目すると、それらに加え EMS の管理画面も確認することができ（図 2）、電力消費量等の状況が表示されるものもありました。

---

i EMS は、Energy Management System の略で、電気使用量の可視化や機器の制御等を行うシステムのことです。家庭向けの HEMS（Home EMS）、商用ビル向けの BEMS（Building EMS）、工場向けの FEMS（Factory EMS）及びこれらを含む地域全体向けの CEMS（Cluster/Community EMS）があります。

ii 23/TCP は、これまでもしばしば増加しており、@police でも注意喚起等を行っています。
「ウェブカメラ等パソコン以外の電子機器をインターネットに接続する際の注意事項について」（平成 25 年 7 月 26 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130726_2.pdf
「2014 年 2 月報」（平成 26 年 3 月 28 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140328.pdf
「2014 年 7 月報」（平成 26 年 8 月 27 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140827.pdf

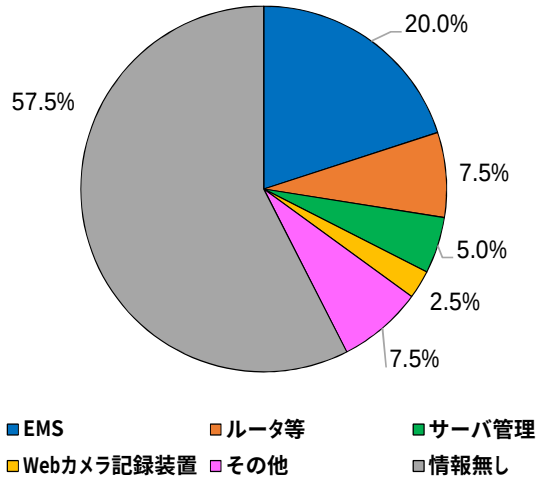

図2　発信元が日本の場合のネットワーク機器等の割合（11 月 1 日～11 月 9 日）

EMS において、識別符号（ID、パスワード等）が安易に設定されていたり、識別符号が設定されていなかったりすると、外部から攻撃者にシステムに侵入され、電気使用量等が閲覧されたり、システムが乗っ取られ、不正に設定変更され踏み台として悪用されたりする可能性が考えられます（図3）。

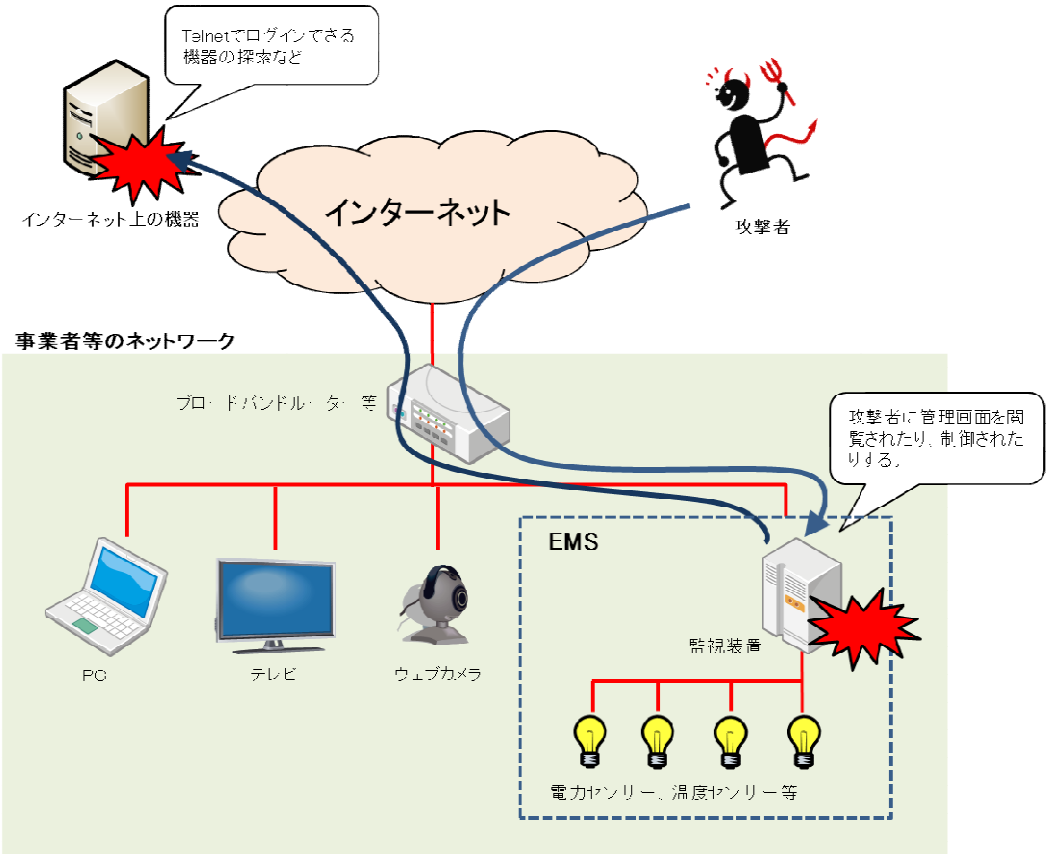

図3　推測されるエネルギー管理システム（EMS）への攻撃のイメージ

3 推奨する対策

最近では、ネットワークに接続できる機器の多くでウェブサーバが稼動しており、ネットワーク経由で設定や管理を行うことができます。これらの機器をインターネットに接続する場合には、以下のセキュリティ対策が推奨されます。

- インターネット側からのアクセスの可否を確認する。
- インターネット側からアクセスを行う場合は、セキュアなプロトコルを用いたり、アクセス制限をしたりするなど、当該機器で可能なセキュリティ対策を行う。
- ログイン ID 及びパスワードは、デフォルトのまま使用せず、推測されにくいものに変更する。