Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 27 年 12 月 9 日

Topic

# 産業制御システムで使用される PLC を標的としたアクセスの観測について

国内メーカー[i] 開発の独自プロトコルを使用する PLC[ii]を標的としたアクセスを継続して観測しています。11 月上旬頃、当該 PLC の起動、停止等の制御を可能とすると思われるツールが公開されました。このことから、システムの管理者は管理する機器の設定を確認し適切な対策を行うことを推奨します。

## 1 国内メーカー製の PLC を標的としたアクセスの観測について

警察庁の定点観測システムでは、平成 27 年1月下旬頃から、産業制御システムで使用される PLC を標的とするアクセスを継続して観測しています（図1）。観測したアクセスは、国内メーカー[i] 開発の独自プロトコル[iii]を使用する PLC に対して接続を要求するものでした。

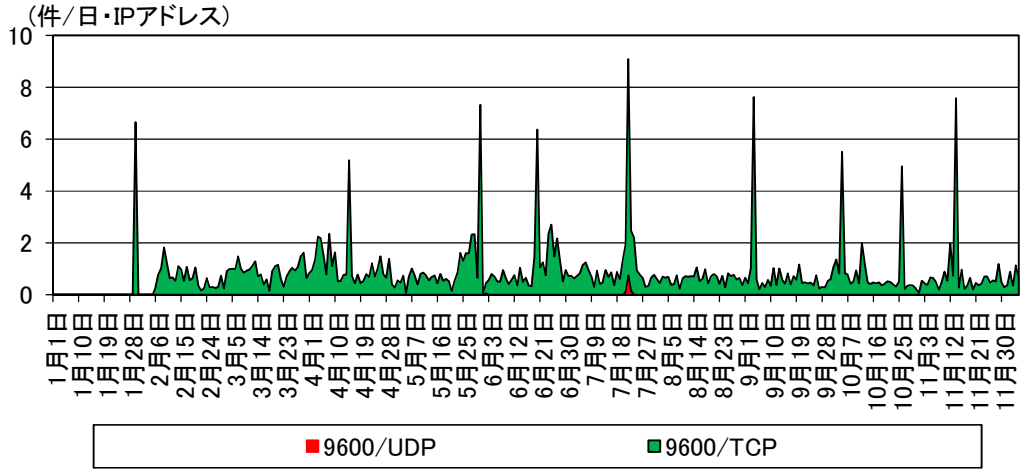


図1 国内メーカー製 PLC を標的とした宛先ポート別アクセス件数の推移（H27.1.1～12.6）

当該プロトコルでは、PLC と機器との間で通信を行うために、標準設定で 9600/UDP 及び 9600/TCP のポートが使用されます。平成 27 年 2 月上旬頃、これらのポートにアクセスして PLC を対象とした情報[iv]を取得するツールがインターネット上に公開されました。また、11 月上旬頃には情報を取得するだけでなく、起動、停止等の制御も可能と思われるツールが公開されたことを確認しています。

---

[i] 「産業制御システムで使用される国内メーカー製の特定の PLC を標的としたアクセスの観測について」（平成27年10月14日）（http://www.npa.go.jp/cyberpolice/detect/pdf/20151014.pdf）における国内メーカーとは異なる国内メーカーである。

[ii] PLC（Programmable Logic Controller の略）とは、プログラム可能なフィールド機器（バルブ、メータ、ファン等）の監視・制御装置のこと。

[iii] このプロトコルは、FINS（Factory Interface Network Service の略）であり、国内メーカー製の PLC で使用されるプロトコルである。

[iv] PLC を対象とした情報には、PLC のモデル番号、バージョン情報等の詳細な情報が含まれる。

観測したアクセスにはこれら公開されたツールの特徴が含まれていることから、当該ツール又は類似した機能を有するツールが使用された可能性が高いと考えられます。

また、これらのアクセスには、インターネット上に接続されている機器に関する情報を収集及びデータベース化し、インターネットからの検索を可能にする Web サービスを提供する組織からの継続したアクセスが含まれていることを確認しています。この検索サービスを提供する組織のウェブサイトには当該 PLC に関する情報が表示されることも確認しています（図2）。

その他、目的が判明しないアクセスも多数観測しています。

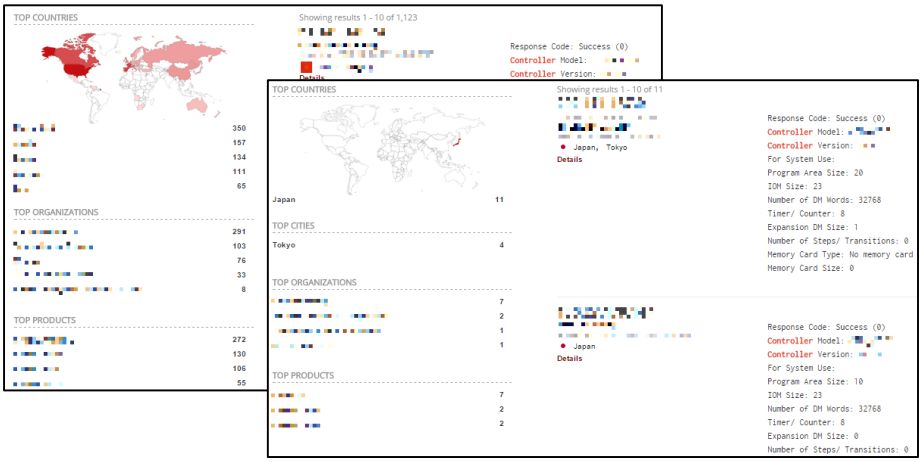


図2　当該 PLC の検索結果

## 2　対策

当該 PLC の情報を取得するツールや制御するツールが既にインターネット上に公開されていることから、これらのツールが悪用される危険性があります。産業制御システムが探索され、システムの停止等の不正な制御が行われると甚大な被害が生じる可能性が危惧されることから、システム管理者は管理する機器の設定を確認し、以下の対策を行うことを推奨します。

- インターネット上からシステムにアクセスする必要がない場合には、インターネットへの不要な公開を停止する。
- インターネット側からアクセスする場合には、不特定の IP アドレスからは接続できないように、適切なアクセス制限を実施する。