平成 27 年5月 26 日

Topic

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

産業制御システムで使用される特定の PLC[i]のソフトウェアにおいて、リモートから任意のコードを実行される危険性がある脆弱性が公開されており、警察庁では当該脆弱性を標的としたアクセスを観測しています。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 産業制御システムで使用される PLC の脆弱性を標的としたアクセスの観測について

平成 26 年 12 月2日に、産業制御システムで使用される特定の PLC のソフトウェアにおいてリモートから任意のコマンドが実行できる脆弱性[ii]が公表されました。また、翌年2月に、当該脆弱性を有する PLC を探索するツールが公開され、5月には、当該脆弱性を利用し PLC の状態を確認するためのプログラム(PoC[iii])が公開されました。

警察庁の定点観測システムにおいては、当該脆弱性を標的としたと思われるこれらのツール等の特徴を有するパケットを観測しています(図1)。

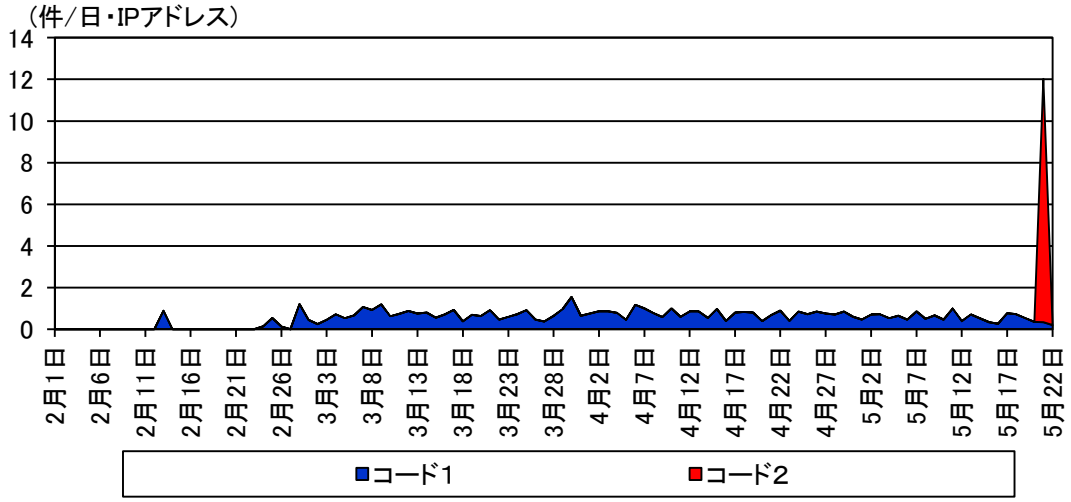

図1 特定の PLC の脆弱性を標的としたアクセスの推移(H27.2.1～5.22)

コード1は、2月に公開された PLC を探索するツールを使用したと考えられるもので、このアクセスの多くは、あらゆるサービスに対して探索を実施して結果を蓄積するとともに、同結果の検索サービスを提供する組織からのものでした。また、この他には、アクセスを行っている者の実体や、その目的について判明しないアクセスも観測しており、同アクセスについて

---

[i] 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。

[ii] 「Phoenix Contact ProConOs および MultiProg における任意のコマンドを実行される脆弱性」 http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-007726.html

[iii] Proof of Concept の略。脆弱性を利用した攻撃が可能であることを示すための検証用プログラムのこと。

は悪用する目的で探索活動を行っている可能性も十分に考えられます。
　コード2は、5月に公開された PoC を使用したと考えられるものであり、このアクセスを行っている者の実体やその目的については判明しておらず、当該脆弱性を悪用する目的でアクセスを実施している可能性も考えられます（図2）。

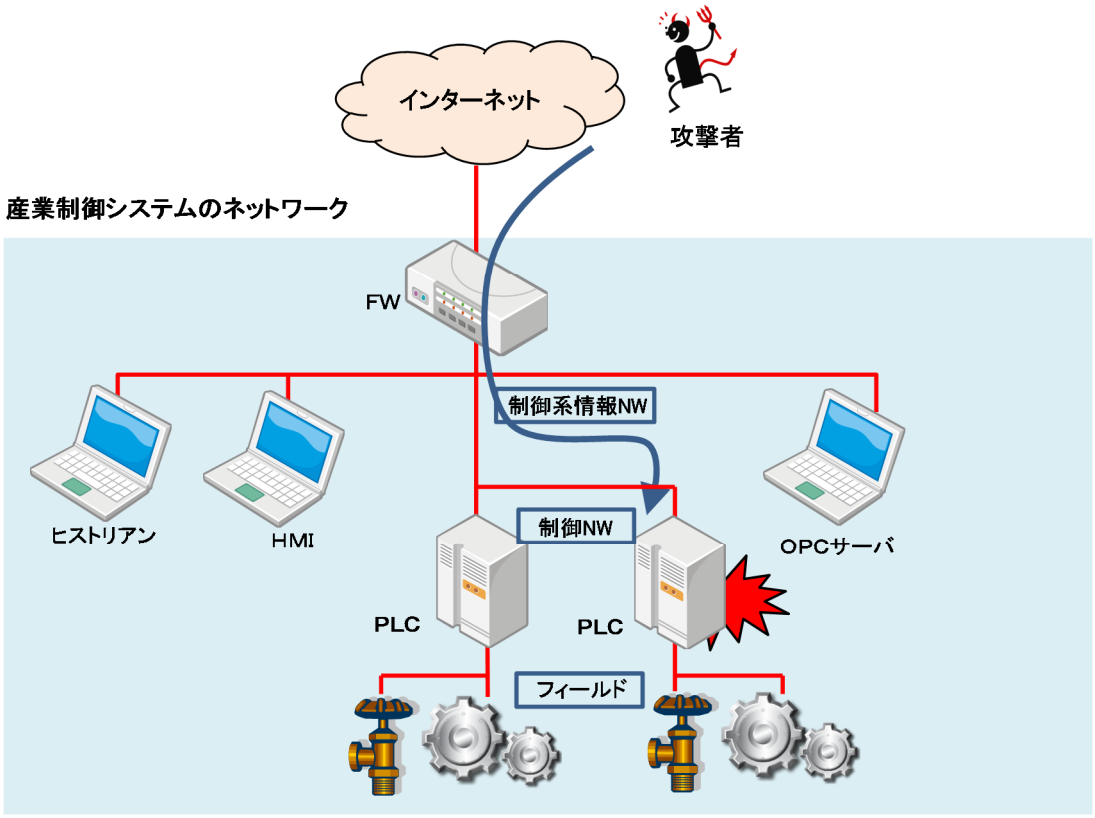

図2　攻撃のイメージ

2　推奨する対策

　産業制御システム等を対象とした攻撃が発生することも懸念されるため、これらのシステムをインターネットに接続する場合には、システムの管理者は、以下の対策を実施することを推奨します。

- 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してください。また、インターネット側からアクセスする場合には、適切なアクセス制限の設定等の対策を実施してください。
- 使用している製品について最新のセキュリティ情報を確認し、必要に応じてソフトウェアのアップデートやハードウェアのファームウェアの更新等を実施してください。