

平成 27 年 6 月 5 日

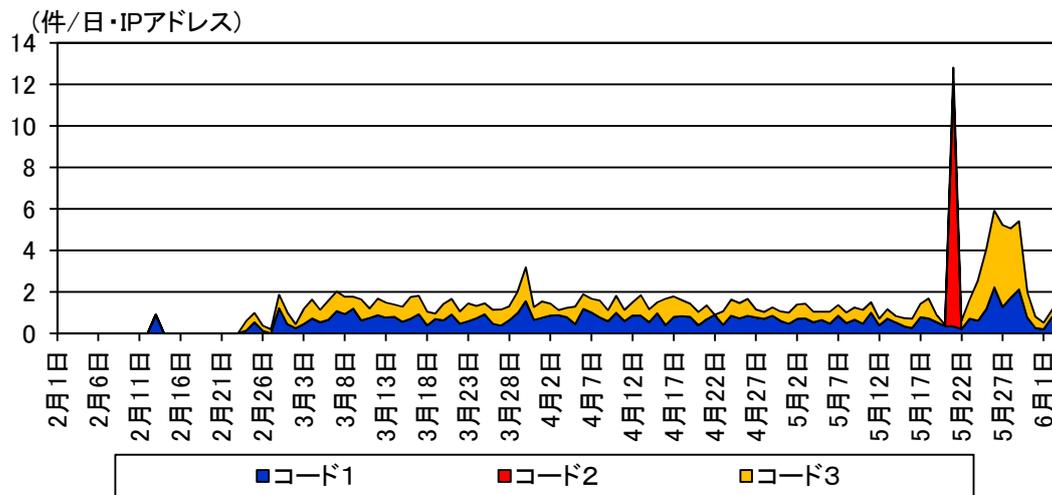
**Topic**

## 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(第2報)

5月下旬から産業制御システムで使用される PLC<sup>i</sup>の探索と考えられるアクセスの増加を観測しました。このアクセスは、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<sup>ii</sup>が存在する PLC を探索するものと考えられることから、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 PLC の探索と考えられるアクセスの増加について

警察庁では、5月下旬から、PLC の探索と考えられるアクセスの増加を観測しました(図)。このアクセスは、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<sup>ii</sup>が存在する PLC を探索するものであると考えられ、平成 27 年 5 月 26 日に@police に掲載した注意喚起<sup>iii</sup>「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」に係る2つのコードとは異なるコードを使用し、標的となるポートも異なるポートに対するものでした。



※コード1、コード2は前注意喚起<sup>iii</sup>で示したコードによるアクセスであり、コード3は今回観測したアクセスを示す。

図 特定の PLC のソフトウェアの脆弱性を標的としたアクセスの推移 (H27.2.1~6.3)

この探索に使用されたと考えられるコードは、2月に公開されており、警察庁の定点観測システムでは、このコードの特徴を有する packets を2月下旬から観測し、5月下旬に増加を

<sup>i</sup> 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。

<sup>ii</sup> 「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/JVNDDB-2014-007726.html>

<sup>iii</sup> 「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 27 年 5 月 26 日)

<http://www.npa.go.jp/cyberpolice/detect/pdf/20150526.pdf>

観測しています。

今回観測したアクセスの発信元の多くは、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、その他には、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、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。

産業制御システムで使用される PLC 等に対する探索活動が、広く行われている可能性があります。

## 2 推奨する対策(再掲)

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ある場合には、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。