JPCERT CC®

# 「制御系プロトコルに関する調査研究」

# 報告書サマリ

有限責任中間法人 JPCERT コーディネーションセンター

平成 20 年 6 月 24 日

JPCERT CC®

# 目次

## １．背景と目的

制御系システムは社会に密着した、われわれの生活に欠かすことができないシステムである。（制御系システムという言葉は用いられる場面により、対象とされる範囲が異なる場合があるが、ここでは、電力システム、ガス、水道、石油化学プラントなど、国民生活の基盤サービスを提供するシステムおよびそれに関連するシステムの意味で用いる）。その制御系システムで利用されているソフトウエアに脆弱性が発見された場合は、生命・身体や重要インフラおよび環境へ直接影響を与える可能性があり、重要な問題となりうる。近年数的にはまだ少ない状況であるが、その制御系システムで使用されるソフトウエアの脆弱性が発見、報告、公開されるようになってきており、その重要性を鑑み、社会的な関心が高まってきている。

これまで発見、公開されている制御系システムに関わる脆弱性には JPCERT/CC 自らが脆弱性情報のハンドリング、公開を行ってきたものが含まれており、その数は増えつつある。それらの脆弱性情報は主として、海外で発見され、海外の関係機関から連絡を受けた脆弱性情報であるとともに、対象としては制御系アプリケーションの脆弱性よりも制御系システムで利用されるプロトコル（以下制御系プロトコルとする）に関する脆弱性がその中心であった。

JPCERT/CC では、このような状況を踏まえ、制御系プロトコルに関して、幅広く調査を行うことが今後の制御系システムに関わる脆弱性の取り扱いを進めるうえで重要であると考え、今回このような調査を実施することとした。

今回公開する報告書の構成は大きく 2 部構成となっており、まず第一部で制御系プロトコルに関する全体像を俯瞰し、第二部で主要な制御系プロトコル（10 プロトコル）に関して詳細な報告を行っている。また、付録(Appendix)として、これまで発見、公開されている制御系プロトコルに関する脆弱性の一覧（12 件）と、一般的な制御系プロトコル(72 種類)の一覧および参考情報を載せている。
制御系プロトコルの調査については、特定の分野、業界を対象とした範囲もしくは、セキュリティにフォーカスしていない一般的な仕様や機能については、既にまとめられたものがあるが、今回の調査のように対象範囲が複数の分野、業界にまたがり全体を俯瞰しえる形での調査でかつセキュリティにフォーカスした調査は実施されていないと JPCERT/CC

では認識している。この調査結果を、制御系システム関係者を含め広く一般に公開することで、制御系プロトコルの現状の認識共有と、日本における制御系システムの脆弱性情報の取扱いのあり方の検討に役立てていきたいと考えている。

# 2．調査内容および調査結果サマリ

## 2.1. 制御系プロトコル概要

### 2.1.1. プロトコルの典型的な利用シナリオ

制御系プロトコルの典型的な使用シナリオについて、デバイスレベル、コントローラレベル、コントロールセンターレベルの制御系システムの階層別にまとめている。

### 2.1.2. 攻撃と脅威シナリオ

本調査で対象としているプロトコルは主として、Ethernet, IP, TCP/UDP ベースプロトコルを対象としているが、その理由をプロトコルへのアクセス、攻撃者のプロトコルに関する知識、攻撃用ツール、サードパーティ製品の脆弱性の影響それぞれのリスクといった側面からまとめている。

## 2.2. 主要制御系プロトコル詳細調査

制御系プロトコルのうち、主要な 10 プロトコルについてその一般的特徴およびセキュリティの特徴について詳細な調査を実施した結果をまとめている。

### 2.2.1. 対象プロトコル

今回の調査では、数多くの制御系プロトコルの中から、主要な標準プロトコル 10 プロトコルを調査対象プロトコルとして選定している。選定にあたっては以下を考慮して対象プロトコルが選定された。

・当該プロトコルの普及度（より普及度が高いもの）
・　プロトコルが使用されている分野・業界（一部の分野・業界にかたよらない方向で選定）
・　プロトコルスタックとして少なくとも物理的に Ethernet を利用しているもの（セキュリティの観点から見た場合に接続性と攻撃ツールの存在といった観点からより大きなリスクが想定されるため）

上記のクライテリアから、調査対象プロトコルとして、以下の 10 プロトコルが選定された。

* CC-Link IE
* DNP3
* EtherCAT
* EtherNet/IP
* FL-net
* Foundation Fieldbus HSE
* IEC 61850
* Modbus TCP
* OPC
* PROFINET

### 2. 2. 2. 調査項目

選定した 10 の制御系プロトコルそれぞれについて、以下の項目について調査を実施した結果を記載している。

・歴史: 当該プロトコルの成り立ち、策定、標準化組織など
・用途: 当該プロトコルのシステム的な利用目的、利用されている分野、地理的な利用状況など
・機能: 当該プロトコルが持つ一般的な機能の特徴およびセキュリティ機能など
・プロトコル実装: 当該プロトコルの実装に関する情報
・他のプロトコルとの関連: 当該システムと他の制御系プロトコルとの関連性(同様なプロトコル、標準化との関連性などを含む)
・脆弱性: 当該プロトコルに関連して公開された脆弱性情報
・攻撃のシナリオと難易度: 当該プロトコルへの攻撃として考えられるリスク、攻撃者へのプロトコルの露出度および定性的な攻撃の難易度
・複雑さ: 当該プロトコルの仕様、実装に関する複雑さ

### 2. 2. 3. 調査結果概要

1)TCP/IP, UDP/IP の使用

10 プロトコルのうち 9 プロトコルが TCP もしくは UDP をサポートしている。CC-Link IE は TCP もしくは UDP モードを持たないプロトコルであり、今回選定した 10 プロトコルの中では最も攻撃の難易度が高いプロトコルであると想定される。EtherCAT および Foundation Fieldbus HSE ではリアルタイム性が要求される用途には、TCP/UDP モードを使用しない。

2)セキュアな領域外でのプロトコルの利用
OPC や OPC UA は異なる制御系システムの相互接続を目的として考えられたプロトコルである。そのため、しばしば Firewall で保護された領域外でも使用される場合があり、攻撃者にとっては魅力的となる場合がある。

3)複雑さとプロトコルへのアクセス
Modbus は非常にシンプルなプロトコルであり、容易に理解して攻撃を行なうことができるが、攻撃者への露出は少ない。一方、Foundation Fieldbus HSE や Ethernet/IP やその他のプロトコルはより複雑であり、オープンソースの実装や当該プロトコルを対象とした攻撃ツールの開発はより困難ではあるが、攻撃者への露出度はより高い。

4)セキュリティ機能の実装
10 プロトコルのうちわずか 3 プロトコルのみがセキュリティ機能の実装を計画している。DNP3 ユーザグループは Secure DNP3 の仕様を策定しており、これらは広く実装されつつある。Secure DNP3 は通信相手の認証とデータの完全性の検証を行う。またこの認証を全部のパケットに対して行なうのかまた一部のパケットにのみ行うのかを設定することが可能であり、セキュリティと性能とのバランスをとることが可能である。IEC 61850 も Secure DNP3 と同様のセキュリティ機能を持っている。

OPC の次バージョンである OPC UA もプロトコル仕様の中にセキュリティが含まれている。しかしセキュリティ機能が実装された製品が出てくるのは 2009 年から 2010 年頃になると考えられている。

他のプロトコルについてはセキュリティ機能の実装は予定されていない。これは制御系システム製品寿命の長さから考えても大きな問題である。

5)プロトコルの実装

10 プロトコルのうち多くがプロトコル実装において独占的、占有的な実装をもっている。例えば、CC-Link の実装には、通常三菱電機のチップが用いられており、また Ethernet/IP の実装には通常 VxWorks 上の Rockwel Automation/WindRiver の実装が用いられている。このことから、これらをターゲットとした攻撃が行なわれた場合には非常に大きな影響が発生することが懸念される。

6)独自プロトコル

制御系システムの脆弱性検査を実施するエキスパートによって、別のベンダの独自プロトコルについて多くの脆弱性が発見されている。これらはほとんどの場合、一般に明らかになることはないが、標準プロトコルの問題とはまた別の大きな問題である。なぜならベンダの独自プロトコルは、標準プロトコルと異なり広く公開されることが少ないため、脆弱性の原因となる問題が、広く検証されずに残されたままになってしまう可能性が高いからである。(このような、ベンダの独自プロトコルの脆弱性が発見される場所は、例えば HMI 操作ステーションとリアルタイムサーバとの通信、リアルタイムサーバと履歴管理サーバとの通信などである)

### 2.3. 制御系システム関連公開脆弱性に関する情報(Appendix A)

制御系システムに関連する、これまで公開された以下の 12 件の脆弱性について情報を掲載している。

* GE Fanuc Cimplicity Heap Buffer Overflow(2008 年 1 月 24 日)
* GE Fanuc Proficy Arbitrary File upload and Execution(2008 年 1 月 24 日)
* GE Fanuc Proficy Plaintext Password Vulnerability(2008 年 1 月 24 日)
* Gesytec Easlon OPC Server fails to properly validate OPC Server handles
* ICONICS Dialog Wrapper Module ActiveX control vulnerability to buffer overflow(2007 年 1 月 2 日)
* ICCP Server heap buffer overflow vulnerability(2006 年 5 月 16 日)
* ICCP Server COTP vulnerability(2007 年 5 月 2 日)
* ICCP Server HTTP/SOAP Heap Overflow Vulnerability(2007 年 5 月 2 日)
* NETxAutomation: NETxEIB OPC SErver fails to properly validate OPC server handles(2007 年 5 月 22 日)
* SISCO: OSI stack fails to properly validate packets(2006 年 9 月 20 日)
* SISCO: OSI stack fails to properly handle malformed packets(2007 年 1 月 17 日)
* Takebishi DeviceXPlorer OPC Server fails to properly validate OPC server handles(2007 年 5 月 19 日)

### 2.4. 制御系プロトコルの概要調査、分類(Appendix B)

制御系プロトコルに関する、おおよその全体像を把握するため、著名な制御系プロトコル（72 種類）について、調査およびその分類を行なった結果を記載している。各プロトコルに関して調査した項目は以下の通りである。

・プロトコル名:当該制御系プトロコルもしくはプロトコルスタックの名称
・カテゴリ:当該プロトコルが用いられるシステム的な階層(デバイスレベル、コントローラレベル、コントロールセンターレベルのいずれか)
・ベースプロトコル:その制御系プロトコルの仕様がベースとしているプロトコル(制御系システムプロトコルの多くは、シリアルベースもしくは IP ベース)
・リファレンス:当該プロトコルの参考情報が参照できる URL
・利用分野:当該プロトコルが主として利用されている分野または業界

### 2.5. 参考情報(Appendix C)

制御系プロトコルに関する有用なドキュメントなどをリストしている。報告書に記載されている内容をさらに詳細に調査したい場合などに有効活用していただくことを想定している。