フィールド機器における脆弱性と脅威

瀬河 浩司　　古原 和邦

（独）産業技術総合研究所
305-8568 茨城県つくば市梅園 1-1-1 中央第二
k.segawa@aist.go.jp　　k-kobara@aist.go.jp

あらまし 時代の要請に対応する形で制御システムのオープン化が進み、情報システムと同様な脆弱性や脅威への対応がせまられている。従来制御システムの中でも隔離度の高かったフィールド機器系統においてもそういった傾向にある。一方、複数ベンダ製の機器や種々のプロトコルを統一的に扱える仕組みも考案／導入されてきているため、ひとたびセキュリティが破られた場合の影響度も激甚化の一途をたどっていると考えられる。ネットワークに接続されたフィールド機器について実際にどのような脆弱性／脅威が存在するのかについて調査した。

Vulnerabilities and Threats in Field Devices

Koji Segawa　　Kazukuni Kobara

National Institute of Advanced Industrial Science and Technology
Tsukuba Central 2
1-1-1 Umezono, Tsukuba, Ibaraki 305-8568, JAPAN
k.segawa@aist.go.jp　k-kobara@aist.go.jp

Abstract With the times, the control system has a tendency to adopt the open architecture. Similar is a field device which is highly isolated from the ordinary control system. On the other hand, a mechanism which can handle multiple ICS protocols uniformly has been appeared. As a result, the influence becomes disastrous once security system is broken. We investigated which vulnerability and/or threat exists concerning a network-connected field device.

1　はじめに

フィールドネットワークについても上位のネットワーク同様オープン化が進んできている。これらにも一般の情報ネットワークで使用されているプロトコルやその上に拡張を施したものが採用されている。一方、従来外部ネットワークから隔離されていたこれらのネットワークが間接的にとはいえ外部ネットワークと接続されるようになってきた。場合によっては直接繋がっている例も増加してきている。しかし、従来隔離された状態にあり、特になにもしなくてもセキュリティ上の問題が発生しにくかったことが災いし、外部から容易にアクセスできる場合でもしかる

べき措置が取られていないことが多い。

2　フィールド機器への攻撃

前項で述べたようにフィールド機器も情報系機器と同様な環境になってきているために、攻撃シーケンスもそのまま、あるいは近い形で適用可能となってきている。一般に、ネットワーク上のシステムを攻撃する場合、『偵察』、『スキャン』、『構成把握』、『実攻撃』などの手順を踏むことが多いが、今や、フィールド機器に対してもこのような方式が有効となっている。特にステップによっては、情報系機器よりも実行が楽な場合さえある。例えば、想定しているターゲット機器の詳細なマニュアルがオンラインでだれでも取得できるようになっている事が多い。こういったドキュメントには、初期設定やネットワークごしの具体的な操作方法などが詳しく記載されていたりする。[1] 仮に、簡易な認証が施されていたとしても、その初期設定ユーザ名／パスワードが「公開」されている状態で、それを放置しておいたり、ひどい場合には変更自体不可能な仕様になっていれば、認証がないのと同じであろう。実際にこういった製品は存在する。ここで強調しておかねばならないのは、その簡便さである。これはハードウェア／ソフトウェアによらない、高度な知識やスキル、経験などがなくても対象システムを容易にクラックできることを示唆している。別の言い方をすると、Stuxnet[2]、Duqu[3]、Flame[4]などといった APT[5]レベルのマルウェアでなくても障害を引き起こさせることが可能ということである。

3　S4 Base Camp による実例

Digitalbond 社の S4 Base Camp プロジェクト[6]で複数ベンダの PLC (Programmable Logic Controller)に対して脆弱性調査が行われた。その結果は、そのホームページにまとめられているが、そこには、その情報をもとに作成された Metasploit[7]のモジュールも公開されており、だれもがダウンロードして使用することができるようになっている。但し、このプロジェクトはもちろんフィールド機器のクラッキングが目的ではなく、あくまでもベンダに対して警告を発し、制御システムの脆弱性をなくしていくという意図で行われた。

3.1　General Electric D20/D20M

ファイル内のコマンド列を記述して tftp で送ると機器がそれらを実行。結果を別ファイルに書き込んでくれる。この脆弱性を使って対話型インターフェイスも提供。また、config データから user, password を取得できる。これをつかって、種々の操作が可能。

3.2　Rockwell Automation ControlLogix

攻撃者が CIP のクライアントシミュレータをつないで PLC にアクセス可能なら、EtherNet/IP CIP のいくつかのコマンド(Ethernetcard や CPU をクラッシュできる。)を認証なしで機器に送ることができる。

3.3　Schneider Electric Modicon

ftpuser, password というアカウント名とパスワードの組でシステム操作用のアカウントとパスワードの組を取得可能。

3.4　Koyo H4-ES

パスワード可能文字列の制限が強いため、ブルートフォースアタックで破ることができる

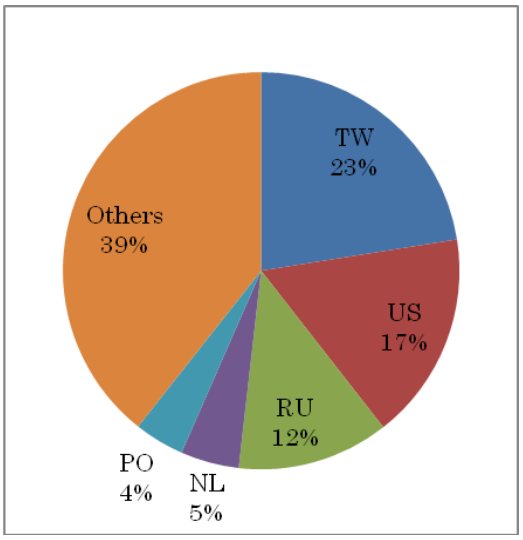
4　SHODAN を用いた情報収集

SHODAN[8]はいくつかのネットワークプロトコルについて、インターネット上から接続できる機器に対してスキャンを行い、特定プロトコルのバナーや DNS などから得た情報をまとめインデクシングしているサーチエンジン。同様のものに ERIPP[9]がある。

このサーチエンジンを活用して実際にどの程度の情報が得られるのか試してみた。

まずある機器をターゲットとし、そのベンダのホームページからドキュメントをダウンロードし、

提供されているサービスやデフォルト設定を調べ、それらを基に複数回にわけて SHODAN で検索をかけてみた。その結果がグラフ1であり、



グラフ1：フィールド機器Aの所在国分布

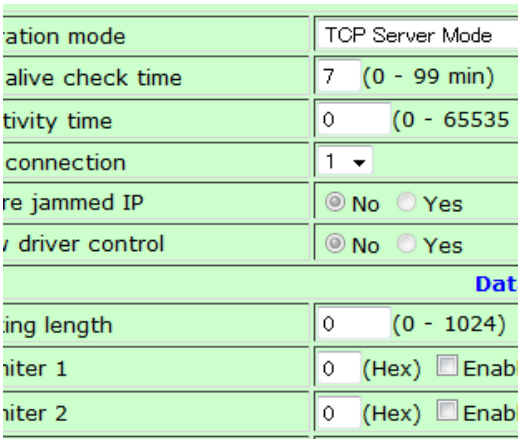
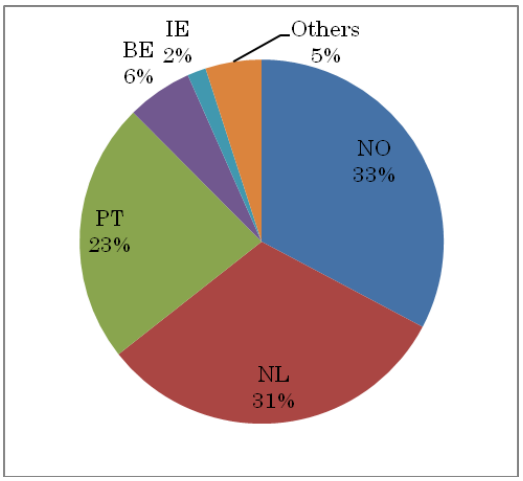


図1：フィールド機器Aへのアクセス画面



グラフ2：フィールド機器 B の所在国分布

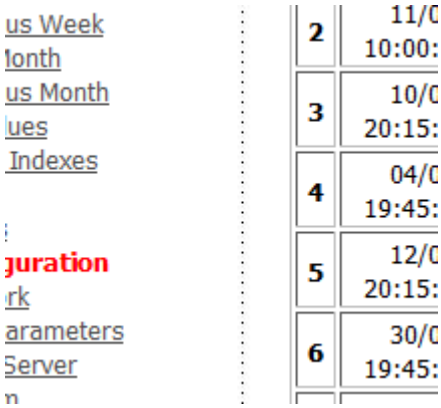
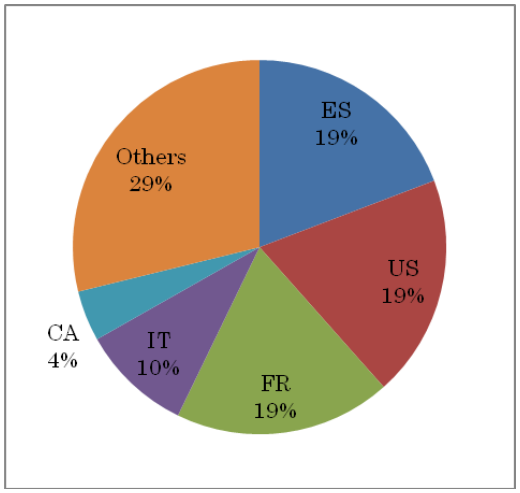


図2：フィールド機器 B へのアクセス画面



グラフ3：フィールド機器 C の所在国分布

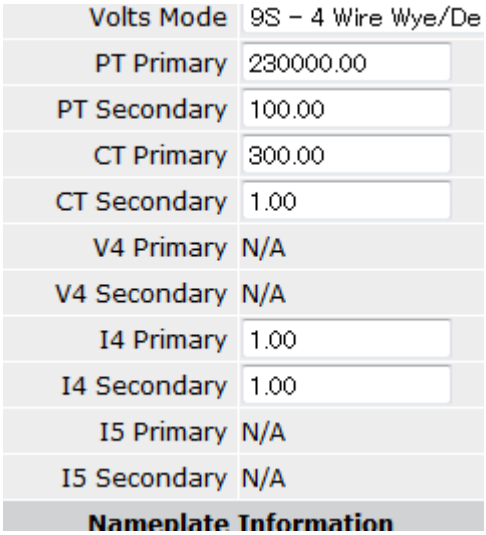


図3：フィールド機器 C へのアクセス画面

検索結果のうちから無作為に選んだ実デバイスにアクセスしてみた結果が図1である。

同様の事を複数の機器についても試してみ

たので同様に結果を記す。

機器Aはシリアルデバイスを Ethernet に接続させるためのネットワーク変換器であるが、世界中で5000台以上が検索で表示され、そのほとんどに対して、認証抜きで接続ができた。この機器はコンソール画面にアクセスできると種々の設定や状態のモニタはもちろん、場合によ手は設定変更も可能である。

分布を見ると、特定の国に偏りがあるものの、アジア、北米、ヨーロッパと広い範囲で使用されていることがわかる。

ハニーポットやダミー／デモ画面の可能性を完全に排除はできないし、実働デバイスであったとしても機器の役割上それほど大きな影響を与えるとは思えないが、セキュリティ感覚への疑問を禁じ得ない。

機器Bはスマートメータ（またはそれへのインターフェイス機器）である。国別分布を見ると西ヨーロッパを中心として普及している機器であることがわかる。

機器A程ではないが認証抜きでコンソール画面にアクセスできるものが多数存在する。ネットワーク設定等対象機器のロケーションを特定する情報へのアクセスには一応認証がかかっているため、数値を読むことができても即座に悪用されるとは限らない。しかし暗号化されていない通信上の Basic 認証しかされていない。しかも使われ方を考えるとアカウント名／パスワードの組みを機器毎に細かく変更していない可能性が高い。つまり一旦どこかで破られると、大きな被害が発生することがあり得る。

機器CはPLCである。国別分布グラフはこの機器が西ヨーロッパから北米にかけて使用されていることを示している。SCADA で使われることが多いようなので、認証抜きで設定情報が見えるだけでも、セキュリティ上好ましくないのであるが、機器Aや機器Bに比べるとさすがにそのままアクセスできる機器は少ない。

以上見てきたように、誰でもアクセスできる情報をもとに SHODAN の表面的使用だけでも十分以上の攻撃対象候補を調べることができた。いずれも情報系機器では以前から言われ続けているセキュリティ上の注意点があまり守られていないことに起因する初歩的な穴の存在がこういった作業を可能にしていることがわかる。・

5 安全系機器

前項までは一般のフィールド機器について述べたが、工場などの制御システムにはもう一系統、安全系統の機器ネットワークが存在する。これは、主に災害発生時に工場を稼働させ続けず即座に停止しなければならなくなった場合、周辺への被害や工場へのダメージを最低限に保ちつつシステムをシャットダウンさせるために存在する。もちろん、通常稼働時における安全確保の目的にも使用される。そのため、従来の安全系統は一般系統とは物理的に別のネットワークで構成されており、ハードウェアもソフトウェアも独自のものが使われていた。

これはその使用目的を考えればもっともではあるが、時代を経て複雑化を増していく制御システムへの対応を困難にせしめる要因にもなっていた。例えば、工場のレイアウトを変える必要がでてきても、リジッドに構成されている安全系統をそれにあわせて容易に変更することができなかった。また現行システムになにか不都合が生じてアップグレードをしたい場合にも同様であった。

時代とともに工場が ERP (Enterprise Resource Planning)などと直接結び付くようになってくると、従来方式では対応しきれなくなってきた。そのために、安全系統と一般系統を同じネットワークで共存させる試みが講じられてきた。産業用イーサネットを拡張して安全バス用のプロトコルとして使用したりしているのもその表れである。

Black Channel 方式を使って実現しているために安全／一般両者が共存しているといっても、少なくとも機能安全面については問題が解消すると言われている。もちろん、安全≠セキュリティなのだが、機能安全を考えればセキュリティに関する問題も発生しにくい方にいくと思われる。しかし、ソフトウェア実装時に重大なバグが

混ざり込んだり、前項で見たように不適切な運用によってシステムが脅威にさらされることは十分ありうる。

本稿では詳しく触れなかったが、こういった事に関しても今後はきちんと見ていく必要がある。

6 まとめ

フィールド機器にはすでに顕在化している脅威が複数確認されている。しかし、そのシステムの性格上、迅速な改良等を行うのが困難なため、また現場のセキュリティに対する認識が低いために、それらが放置されたままになっている場合が多い。現在、インターネットから直接アクセスでき、かつセキュリティ上の対策が甘い機器についての一般的なリスクアセスメントは困難であるが、リスク自体は確実に存在している。また、こういった状況を踏まえ、新たに対策を考慮しつつ作り上げられた新しいプロトコルやシステムについても実装や運用上の面において脅威が完全に取り除かれたとはいえない。今後、攻撃のターゲットは、より下のレベル、そして安全系機器へと移行していくことは明らかである。特に安全系機器への攻撃は一たび成功すると被害の激甚化がさけられないため、脅威やリスクに関する解析は重要であると考えられる。まずは誰もが仕様を読むことができる openSAFETY[10]のようなプロトコル等についてこういった調査・解析を試みる予定である。

参考文献

[1] NIST SP800-82
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[2] W32.Stuxnet
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2010-071400-3123-99

[3] W32.Duqu
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2011-101814-1119-99

[4] W32.Flamer
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2012-052811-0308-99

[5] "Advanced Persistent Threat (or Informationized Force Operations)". Usenix, Michael K. Daly. November 4, 2009. Retrieved 2009-11-04

[6] S4 Base Camp Project
http://www.digitalbond.com/tools/basecamp/

[7] Metasploit
http://www.metasploit.com/

[8] SHODAN
http://www.shodanhq.com/

[9] ERIPP
http://eripp.com/

[10] openSAFETY
http://www.open-safety.org/