MOF2008 パネルディスカッション

産業用イーサネットのイントラ接続の可能性と相互接続を考える

～制御系システムセキュリティとサイバーセキュリティ～

JPCERTコーディネーションセンター
業務統括
伊藤　友里恵

2008/09/12

はじめに:
先週のCitect SCADA製品の脆弱性をつく攻撃コード出現の事例から

制御系システムの脆弱性をつく侵入コードの一般公開まで

制御系システムの脆弱性をつく侵入コードの一般公開まで

JPCERT CC®

- **2008-01-30** : 発見者である研究者チーム(Core Technologies)が、ベンダーにコーディネーション開始
- **2008-06-11:** Security advisory CORE-2008-0125 published.
- **2008-06-12:** CERT、JPCERT/CC アドバイザリー公開
- **2008-09-05:** 当該脆弱性をつく、侵入コードがメタスプロイトで公開

キーポイント

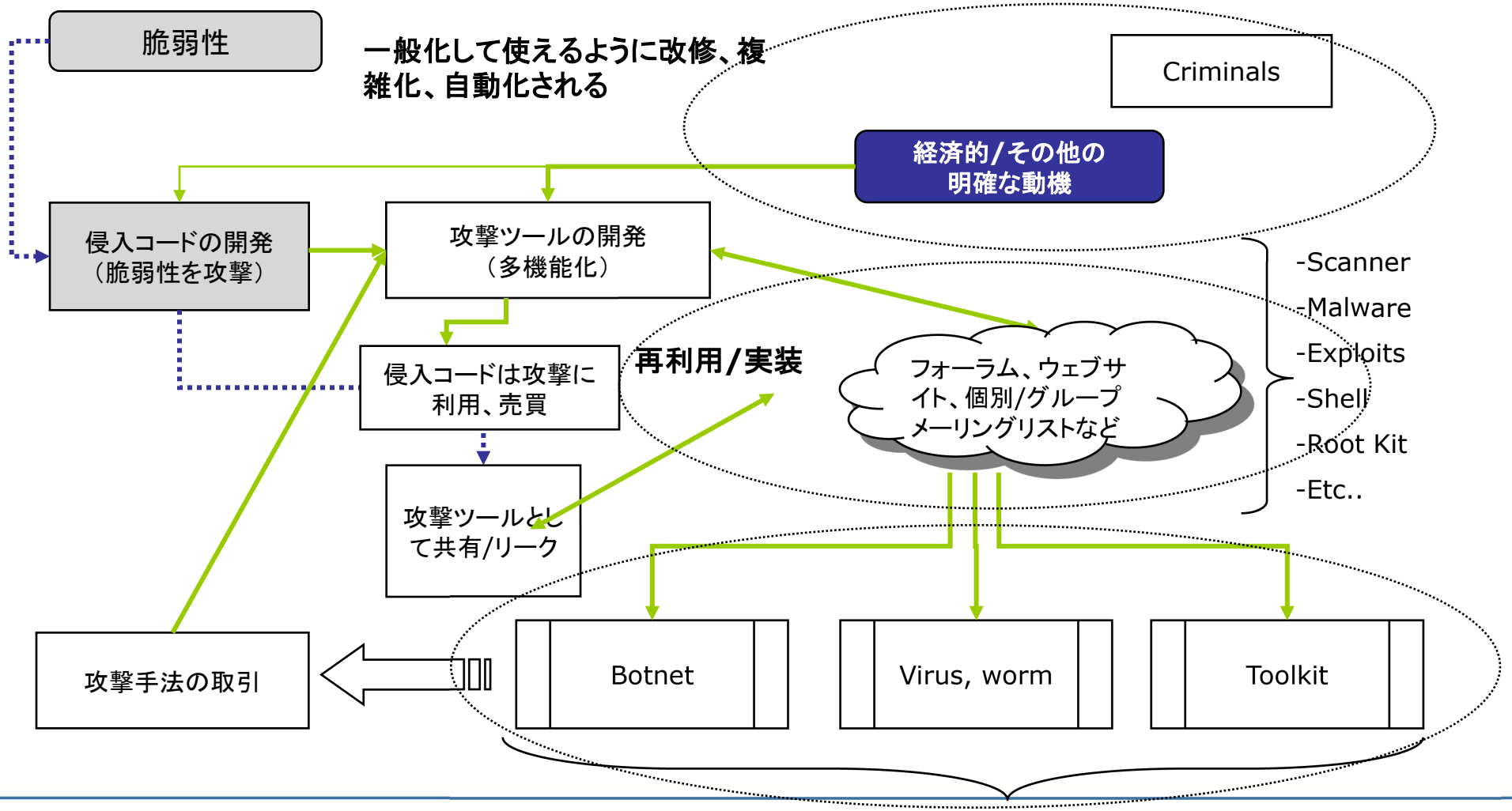
- 制御系システムの脆弱性でも、情報は公開される
  - 検証コード
  - コーディネーション履歴

  ベンダーも、事業者も、脆弱性通知の連絡に対応できる体制の準備が必要

- メタスプロイトとは
  - フリーのオープンソース 侵入コード
  - 侵入テスト、ハッカーコミュニティに利用される

  ハッカーコミュニティが、制御系システムへの関心を高めている
  今後も、侵入コードは世の中に出回ることになる

攻撃者コミュニティにおける脆弱性、マルウェアの売買取引



脆弱性情報オークションサイト、取引サイト

JPCERT CC®

WabiSabiLabi
CLOSER TO ZERØ RISK

制御系システムネットワークと、情報系ネットワーク

JPCERT CC®

- 制御系システムネットワークのオープン化が進んでいる
  - アプリケーション、PC、サーバーを汎用Unix、Windows OS上で稼動させる
  - データベース、ウェブアプリケーション、TCP/IP、Ethernet利用の増加
  - PLC、RTU、フィールドデバイスのほとんどの製品は、EtherNET、IEのインターフェースをオプションとして持つ
  - さらに多くの装置
  - 無線LAN、WANの増加

制御システムは、攻撃を受けやすくなり、脆弱なファクターも増加

事業者における適切なセキュリティ対策が必要である

それでもまだ制御系システムがつながっていない!?
http://blog.wired.com/27bstroke6/2008/08/virus-infects-s.html

JPCERT CC®

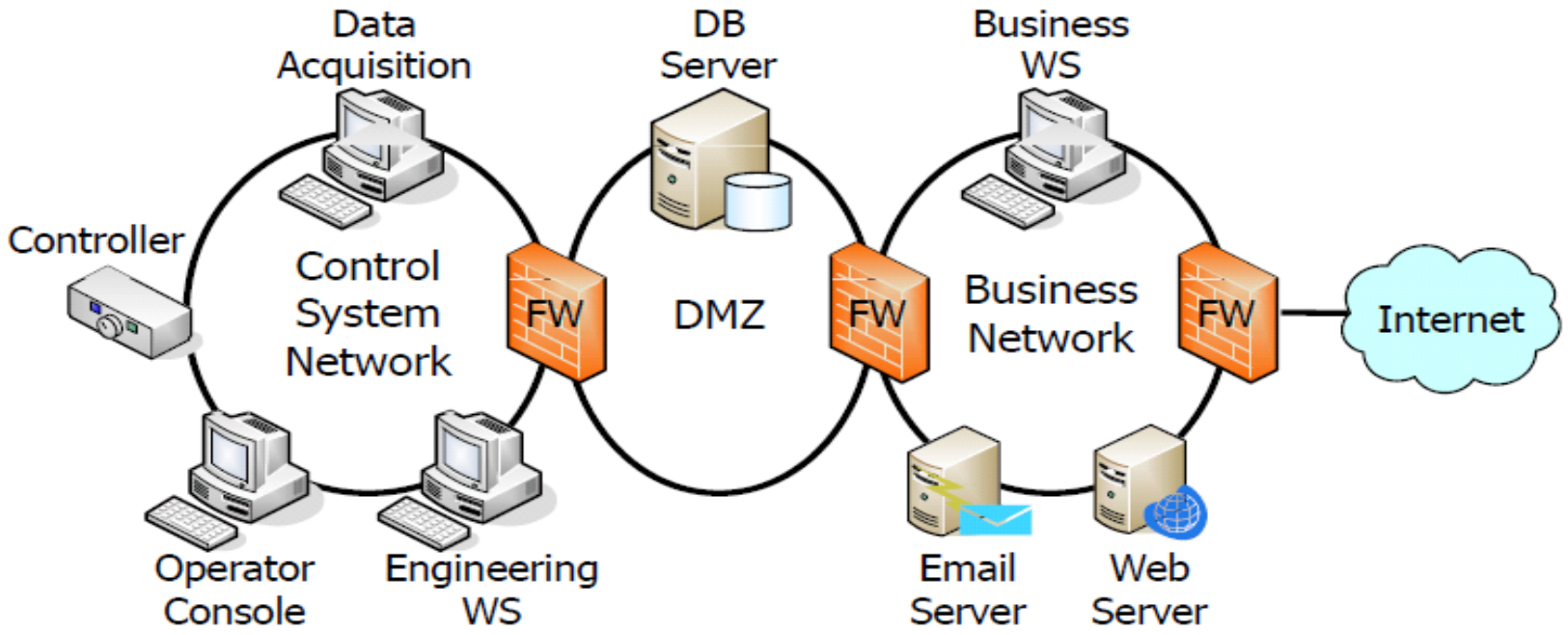
ブログ記事については、掲載省略

ネットワーク境界セキュリティの穴

電中研の資料から：制御系システムの構築例の一つ

JPCERT CC®

SCADA System Architecture



ファイヤーウォールによるネットワークセグメンテーション

JPCERT CC®

- **ベストプラクティス実装してますか?**
  - 多層ファイヤーウォールの実装
  - 最小特権の実装。全てを拒否するところから開始して、ファイヤーウォールの設定を行う。ファイヤーウォールに穴を開けるということは、その穴がセキュリティ上の攻撃ベクターになるということ。本当に必要なサービスかどうか確認。
  - 内側と、外側の(非セキュア層から、セキュア層への)直接のコネクションを絶対に許さないこと。全てのパスはDMZを介するように設定する
  - データはプッシュ型で
  - TCPはUDPよりベター
  - 最少数の穴をあけること、穴を空ける場合、それがまちがいなく必要な穴だということを評価すること。
  - ルールベースを定期的に見直す

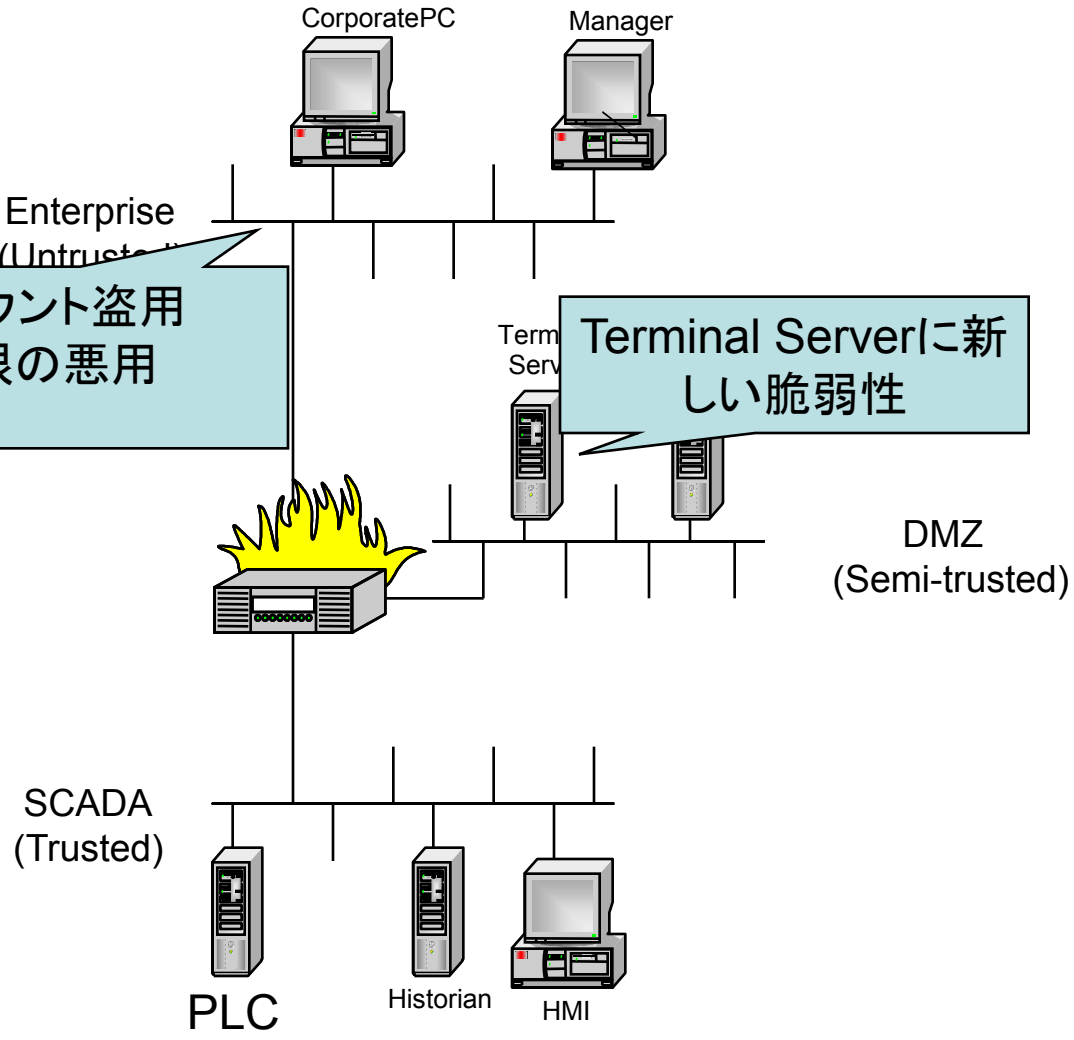
ファイヤーウォールによるネットワークセグメンテーション

JPCERT CC®

- **システム復旧のための緊急遠隔アクセスを除けば、どんな場合においても、プロセス制御部分は、企業ネットワークもしくは、非セキュ[illegible]ワークからのアクセスを許し[illegible]けない。**

- 現実に散見されるシステム構成：

PLCとフィールドデバイスのメンテナンスを、企業内ネットワーク上のPCから行おうとするもの



境界セキュリティ：ベストプラクティス（続き）

JPCERT CC®

- 複数のDMZ層を持つこと
  - 適切にポリシ分けした、異なるユーザーコミュニティ向け
  - ひとつのDMZは履歴情報にアクセスする担当者用、別のDMZ層は、緊急遠隔アクセスのための管理者アクセス用など

システム構成上ひとつ以上のDMZを設置することを考慮し、その際はユーザーコミュニティの確認、承認レベル、許可する通信など、ポリシーをきちんと確認すること

- IPS

  一般的に、IPS（侵入検知システム）は、制御システムに実装されていないが、ほとんどのファイヤーウォールはその機能をサポートしている。パッチのテストと実装の遅延に関する対策としてIPSを利用することを考慮することができる。

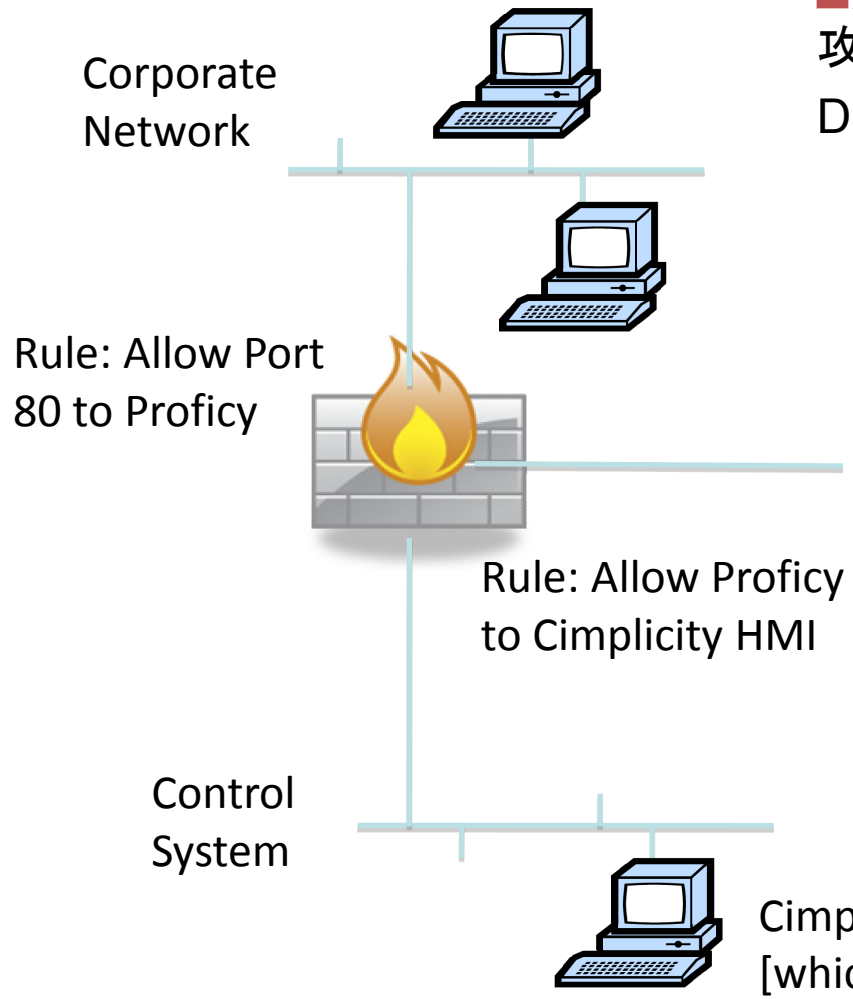
承認されたファイヤーウォールの穴も攻撃ベクター

JPCERT CC®

- 完璧なファイヤーウォールを構築していても、全てのファイヤーウォールの穴は、攻撃ベクターである。
  - ファイヤーウォール越しに提供されるサービスに、侵入可能なバグがある場合、攻撃者はファイヤーウォールを通り抜けることができるから
- 完璧に設定されたファイヤーウォールを介して、企業ネットワークから、脆弱性を利用して、制御系システムに攻撃をかけた例
  - by イスラエルの研究者のEyal Udassinのデモ、S4カンファレンス

Eyal Udassinのデモ、S4カンファレンス

■適切に設定されたファイヤーウォールを介して、攻撃者が企業ネットワークからSCADAもしくは、DCSをコントロールできるということの証明



ネットワーク境界セキュリティの穴

JPCERT CC®

- 全てのファイヤーウォールの穴は、その先のサービスに脆弱性があれば攻撃ベクターとなる可能性があること

- 多層防御は必要。ファイヤーウォールに全てを依存してはいけない。
  - AV、認証/承認、モニタリング、検知などを組み合わせる

- **JPCERT/CCからの脆弱性情報の通知を受け取れるようにすること。**

  JPCERTは、国際的なネットワークを通して、全世界から脆弱性情報の連絡、調整を行っています。ベンダのPOC、事業者のPOCを登録いただけば、情報展開することができます。

制御システムプロトコルスタックの脆弱性

制御システムプロトコルスタックの脆弱性

JPCERT CC®

- 多くの制御システムプロトコルスタックは脆弱
  - 意図されていないデータがデバイスやアプリケーションに送られてクラッシュ
  - 制御システムの一部か全体に影響を及ぼすことも
- 単純なポートスキャンが、制御システムをクラッシュさせるという事例は数多く見つかった。

ブラウンフェリー原子力発電所 の緊急停止

- 2006年8月16日、米国のブラウンフェリー原子力発電所のユニット3が緊急停止
- 冗長化してあるPLCの全てが同時に落ちたことによって緊急停止に至った。
- このPLCは、リアクターを冷やすための冷却水の循環を制御する装置として使われている
- ここでの問題でリアクターが冷却されなかったことによって緊急停止となった。
- 事故調査は、PLCのEthernetインターフェースに対して、想定以上のトラフィックが送られたことが原因だったと特定した。
- 直接的で意図的な攻撃のエビデンスは見られていない。
- ネットワーク上の他のデバイスがフェイルしてブロードキャストトラフィックを送信したことにより、PLCのプロトコルスタックが処理し切れなくなって、落ちたと検証された。

このインシデントから学ぶこと

- どんなトラフィックが制御ネットワークに流れるのか、制限、管理することが必須
- 攻撃トラフィックだけはなく、さらに第3者の開発したアプリケーションなども、きっちりとテストするまでネットワークにのせない
- セキュア制御システムプロトコル
  - 望ましくは、制御系システムの全てのリクエストと応答は、全てソースと、データの完全性を認証すべき。ただし、この機能は今日ないために、適切なクライアントソフトと、制御システムの知識があり、境界に侵入することができる能力の高い攻撃者は、送信中の全ての制御データを見て、プロセスを変更することができる。
  - 良いニュースは、セキュアDNP3、OPC UAとIEC62351-5 といった、プロトコルレベルでソースとデータの認証を行うものが出てきていること。
  - 製品として実装されるには、まだ時間がかかるものの、他のプロトコルにもこのような動きが始まることが期待される。

JPCERT/CC、Digital Bond プロトコルセキュリティ調査

- 制御系プロトコル概要
  - 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。
  - 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。

JPCERT/CC、Digital Bond プロトコルセキュリティ調査

JPCERT CC®

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。

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

- ・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

JPCERT/CC、Digital Bond プロトコルセキュリティ調査

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。CCLink、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。

JPCERT/CC、Digital Bond プロトコルセキュリティ調査

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。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。

JPCERT/CCの取り組み： 脆弱性対応と、啓発活動

JPCERT CC®

JPCERT CC®
有限責任中間法人 JPCERT コーディネーションセンター

一歩先の信頼と安全を提供するために

Japan Computer Emergency Response Team Coordination Center | English

Home > 公開情報 > 制御系システムセキュリティ > プロセス監視・制御系システム、SCADAセキュリティ

Contents

JPCERT/CCについて

- 代表理事あいさつ
- 組織概要
- JPCERT/CCに関するFAQ
- 活動概要
- 採用情報

インシデント対応

- フィッシング FAQ
- インシデント報告の届出
- PGP公開鍵 (http)
- PGP公開鍵 (https)

脆弱性情報ハンドリング

- 製品開発者リスト

プロセス監視・制御系システム、SCADAセキュリティ

最終更新: 2008-08-26

制御系システムは、製造業を含むさまざまな産業領域で利用されている他、大規模な石油化学プラントの制御や、電力システムの監視制御、ダムや水供給システムの監視制御など国民生活の基盤サービスを提供する重要なシステムとして利用されています。その一方で、制御系システムに関連するソフトウエアに脆弱性が発見されるという事案も散見され始めています。

JPCERT/CC では、脆弱性関連情報調整機関として、プロセス監視・制御系システムにおける

開発者、研究者との情報共有タスクフォース (準備中)
脆弱性情報の通知、対策調整
脆弱性情報の情報公開
制御系プロトコルに関する脆弱性調査
プロセス監視・制御系システムセキュリティに関する各種情報収集
プロセス監視・制御系システム運用者への早期警戒情報発信 (準備中)

制御系システムベンダー・研究者情報共有タスクフォース

JPCERT CC®

- JPCERT/CC 脆弱性対応POC登録ベンダーフレームワーク
  - 制御系システムベンダー・研究者情報共有タスクフォースの発足を予定（2009年2月目標）
  - 制御系システムセキュリティに関する問題の調査、共有
  - 脆弱性関連情報の共有
  - 当該脆弱性のインパクト、情報公開方法の協議

お問い合せ

- プロセス監視・制御系システム、SCADAセキュリティ について
  - Email: scada@jpcert.or.jp
- インシデント対応依頼、インシデント情報のご提供は
  - Email: info@jpcert.or.jp