JPCERT CC®

国内の制御システムにおける汎用通信プロトコルの利用状況およびセキュリティへの取組み状況に関する調査

一般社団法人 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

現代社会において情報システム、情報通信ネットワークはすでになくてはならないものであり、一般国民から企業、政府まで幅広く活用されそのメリットを享受している。企業においては会計・業務システム等の基幹系システムの他、顧客管理、生産管理、売上管理に至るまで積極的に情報化を進め、コスト削減、サービス価値向上へ向けてのライフサイクルを構築し競争力の強化に努めている。

制御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が、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システムとして利用されることも多い。従来こういった制御システムはプロプライエタリなシステムとして開発される場合が多かったが、特に欧米諸国では、制御システムのオープン・システム化、汎用ソフトウエアの採用が急速に進み始めている模様である。これに対応して、制御システムのセキュリティ確保が必要との共通認識から、研究団体やセキュリティベンダーによる、制御システムの脆弱性に対する研究・取り組みが行われている。その背景には、制御システムの脆弱性は、国民の生活基盤に密接に関係する問題であり、ひとたびその脆弱性が悪用されると、身体・生命・財産に直接影響を与える可能性があるという認識があると考えられる。

国内の制御システムのオープン・システム化の状況を見ると、「大規模プラント・ネットワークセキュリティ対策委員会（PSEC）」最終報告書[1]（1999 年 3 月、通商産業省）ですでに指摘されているとおり、大規模なプラントの制御システムを対象に、標準プロトコルを用いたオープン・システム間の相互接続が進展してきている。昨今では、ビル制御システム分野についてInterop2005 内“ファシリティネットワーキングShowcase”においてマルチベンダーによるIPv6 を活用したビル管理システムの遠隔監視・制御デモが行われ、製造業分野で技術標準化団体の連携によるフォーラム“Manufacturing Open Forum 2004/2006”が開催され導入事例や活発な技術情報の交流が見られた事例に示されるように、プラントのみならず産業・制御システムにおけるオープン・システムの活用が幅広い関心を集めており、今後さらに採用が進むと予想される。

このような状況の中、制御システムに関連する脆弱性が散見され始めている。国際的な枠組みで脆弱性情報の交換を行っているJPCERT/CC では、海外の脆弱性情報取扱い組織から 2006 年度に初めて制御システムに関する脆弱性情報の報告を受け、2008 年 2 月までに計 13 件の脆弱性情報を取り扱いＪＶＮ(Japan Vulnerability Notes)[2]上で公表した。通常の情報処理分野の製品に比してまだ件数は少ないものの、オープン化の進展に伴って今後も増える可能性が高いと予測される。また、公表された脆弱性に対する対策も、PC 用のソフトウエアに対する対策と比較して、時間がかかる、あるいは難しいケースが大多数

[1] http://www.ipa.go.jp/security/fy11/report/contents/intrusion/psec/index3.html
[2] http://jvn.jp/

であることも懸念されている。

本調査を行った目的は、調整機関として国内で利用されている制御システム関連製品に関する脆弱性情報の届出が行われた場合、できる限り的確に影響を推定し、製品開発ベンダや製品利用業界などとの調整活動を円滑かつ取りこぼしなく進めるための基礎資料を得ることにあった。

2. 検討にあたって

本調査では実践的な知見を得るという観点から、調整機関として、今後の制御システムに係る脆弱性情報の分析とその取扱いを円滑かつ取りこぼしなく進めるための要件を下記１，２と定義した。

1) どのような団体がこの分野の知見を持つのか理解すること
   (ア) 制御システムの脆弱性の脅威度分析の観点から必要な時に適切な助言を得られる団体を把握しておくこと
   (イ) 調整業務を円滑に進めるための研究、を行っていくため既存研究成果を活用すること
2) 国内において､オープン規格の通信プロトコルが採用された製品がどの程度利用されているのか把握しておくこと（影響範囲の推定）
   (ア) 官・学・民で活用可能な研究・調査を把握すること。

そのうえで、上記要件を満たすための調査として、以下の 2 つの項目についての調査を実施した。

A) 国内の制御システムの通信コンポーネントにおける汎用プロトコルの利用概観の調査
B) 国内の制御システムに関するセキュリティ活動の取り組み状況調査

調査 A）における製品の利用状況については、市場調査（マーケティング・リサーチ）によって実施するのが一般的である。しかし、それらは企業戦略上の意思決定の材料を目的としているのに対し、本調査は脆弱性情報の脅威分析と影響範囲の推定に主眼が置かれているため観点が異なっている。また、コスト・正確性・セキュリティ面から、製品開発者を対象とした本格的な調査を実施する場合には、調査対象者への一層の配慮が必要である（個別企業の製品利用情報が攻撃者に知れると、脆弱性情報の悪用に利用される可能性があるという指摘）という意見もあるなど、解決すべき課題も残っている。従って、本調査では市場調査資料と公開情報等を活用しながら関係者へのヒアリングを行う手法をとった。

3. 調査時期・方法・体制

3.1 調査時期

平成 20 年 1 月～3 月

3.2 調査方法

調査は以下の方法で実施した。

1) ヒアリング

・製品開発ベンダ、制御システム関連研究者

・国内制御システム関連団体

2) アンケート

プロトコル推進団体を対象に行った。

- ＭＥＣＨＡＴＲＯＬＩＮＫ協会
- ＯＤＶＡ　日本支部
- ＣＣ－Ｌｉｎｋ　協会
- Ether CAT　Technology　Group
- 社団法人日本電機工業会（FL-net）
- 日本　ＡＳ－ｉ　協会
- 日本プロフィバス協会
- NPO 法人日本フィールドバス協会
- 日本 OPC 協議会

3) 調査資料の活用

以下の資料を参考とした。

・　「産業用 Ethernet 関連機器の業種別ニーズ実態と市場展望」（2007 年 2 月、株式会社富士経済）

・　「エンベデッドシステムマーケット 2008」（2008 年 3 月、株式会社富士経済）

・　「ビルオートメーションシステムにおける IP 化・オープン化関連市場実態調査」（2007 年 9 月、株式会社富士経済）

・　「2007 リモート監視関連市場徹底総調査」（2007 年 7 月、株式会社富士経済）

・　電気設備学会誌 Vol.27　（2007 年 12 月、社団法人電気設備学会）

3.3 調査体制

一般社団法人　JPCERT　コーディネーションセンターで行い、必要な場合に有識者から意見を頂く形で行った。

4. 調査結果概要

A) 国内の制御システムの通信コンポーネントにおける汎用プロトコルの利用概観

制御システムで利用されるプロトコルは、産業領域ごとに標準化されているもの、事実上標準となっているものも含め多くのプロトコルが存在する。今回の調査では、あらかじめ用意したプロトコルのリストの中から国内の利用概観をつかむために確認が必要と思われるプロトコルを優先的に取り上げ、関係者へヒアリングすることとした。

○ヒアリング結果

制御システムの通信プロトコルのうち、海外に比して日本国内の利用割合が高いと推測されるプロトコルは **CC-Link** と **FL-net（後述）**であった。このプロトコルは国内製品開発者が中心となって普及に努めており、日本や近隣アジア各国でも利用が進んでいる。

○プロトコル推進団体の確認

多くのオープンなプロトコルには非営利団体・ベンダ会・ユーザ会といった形で、普及啓発・ライセンスや技術情報の管理・相互運用性に関する情報提供、等のための組織が存在する。そのうち日本国内で支部などが設立されているものは、利用が進んでいるか注力していると思われるため、アンケートを行った。

但し、アンケートを行ったところ、すべてのプロトコル推進団体から「国内で利用されているユーザ数は正確に把握していない」又は無回答であったため、欠測とした。

表 1

団体名	プロトコル名
ＭＥＣＨＡＴＲＯＬＩＮＫ協会	MECHATROLINK
ＯＤＶＡ　日本支部	Common Industrial Protocol (CIP)
	ControlNet
	DeviceNet
	Ethernet/IP
ＣＣ－Ｌｉｎｋ　協会	CC-Link
Ether CAT　Technology　Group	Ether CAT (Ethernet for Control Automation Technology)
社団法人日本電機工業会	FL-net (OPCN-2)
日本　ＡＳ－ｉ　協会	Actuator-Sensor (AS) Interface
日本プロフィバス協会	PROFIbus、PROFInet
NPO 法人日本フィールドバス協会	Foundation Fieldbus/H1

	Foundation Fieldbus/HSE
日本 OPC 協議会	OPC
	OPC UA

○市場調査資料から

・　　産業用 Ethernet 技術の進展

海外を中心に Ethernet 技術はオフィスにとどまらず制御システムでも利用が進みつつあり、標準規格として IEC/TC65/SC65C の WG11 と MT9 によって標準化作業が進められている。国内においても、実績は少ないが三菱電機「MelsecNetG」、オムロン「Ethernet/IP 対応 PLC ユニット販売」など販売が始まるなど、徐々に産業用 Ethernet の国内利用状況は変化していくと思われる。産業用 Ethernet の主なニーズとしては、大容量のデータ通信があり、その制御システムにおける用途としては「プロセスデータ管理」「遠隔監視・制御ニーズ」「フィールド機器のインテリジェンス化」の他、「無線 LAN」「海外からの影響」「(XML を利用した) 複数規格間の接続」といったニーズがある。(『産業用 Ethernet 関連機器の業種別ニーズ実態と市場展望』(2007 年 2 月、株式会社富士経済) より)

・　　組込み機器向け通信機能へのニーズ

組込み製品向けの OS、ミドルウェア、の高機能化に伴いネットワークへの対応ニーズが高い。そのため、TCP/IP や IPSec/SSL 等の通信コンポーネント採用は徐々に広がりを見せている。組込み製品そのものは本調査のテーマとは離れるが、Windows や Linux などの汎用 OS 以外の領域でも標準化・規格化された通信プロトコルを採用した製品の利用が進んでいる点を留意しておきたい。(『エンベデッドシステムマーケット 2008』(2008 年 3 月、株式会社富士経済) より)

○産業分野からみた状況

・ビル・オートメーション分野

ビル・オートメーション分野のシステムは IP 化・標準化・オープン化が進んでおり、システムに採用されている通信プロトコルに関しても同様である。藤原憲明「ビルオートメーションシステムにおける統合ネットワーク」(2007 年、電気設備学会誌) によると、「ASHRAE」(米国暖房冷凍空調学会)、「BACnet」(米国標準規格) と「LonWorks」(エシュロン社) が主なプロトコルのようである。

○その他国内の動向がわかる活動など

国内の関連セミナー、ワークショップ、シンポジウム(オープンなもの)

・　　JEITA　産業社会制御システムフォーラム(社団法人 電子情報技術産業協会　主

催)

・ Manufacturing Open Forum （IA 懇談会 主催）

・ SICE Annual Conference（社団法人 計測自動制御学会 主催）

・ 重要インフラ情報セキュリティセミナー （独立行政法人情報処理推進機構、一般社団法人 JPCERT コーディネーションセンター共催）

B) 国内の制御システムに対するセキュリティ活動の取り組み状況

制御システムセキュリティについて研究活動を行っている国内の主要な団体は下記であった。

・ JEITA[3](社団法人 電子情報技術産業協会)制御システム専門委員会セキュリティ WG

・ JEMIMA[4](社団法人 日本電気計測器工業会)セキュリティ調査・研究WG

・ SICE[5]（社団法人 計測自動制御学会）計測・ネットワーク部会

上記団体は相互に協力がなされ協働して成果発表を行っている。なお、上記の団体とは別に、電力システム分野においては電力中央研究所が研究活動を進めている。

過去にさかのぼると、「大規模プラント・ネットワークセキュリティ対策委員会」（１９９７、通商産業省 6）においてサイバーテロ対策の観点から制御システムセキュリティも含めたプラントシステム全体のセキュリティ対策について幅広に議論がなされている。

5. 国内の制御システムにおけるオープン化の動向

制御システムはいくつかの階層に分けることができ、上位から、①情報システム・ネットワーク又はコンピュータレベル（以下情報システム）、②制御システム・ネットワーク、コントローラレベル又はコントロールバス（以下制御システム）、③デバイスレベル（以下デバイスレベル）、と呼ばれることが多いようである（あくまで代表的な分類であるため実際のシステム構成が必ずこの形になっているという説明ではない）。本調査のテーマである制御システムの調査では②の領域を中心としている。（①は企業内システムと同等であるため、そこで使われる製品で一般に利用され入手可能な汎用ソフトウエアの脆弱性についてはすでに取組みが進められている領域である。）

[3] http://www.jeita.or.jp/japanese/
[4] http://www.jemima.or.jp/
[5] http://www.sice.or.jp/
[6] http://www.ipa.go.jp/security/fy11/report/contents/intrusion/psec/index3.html

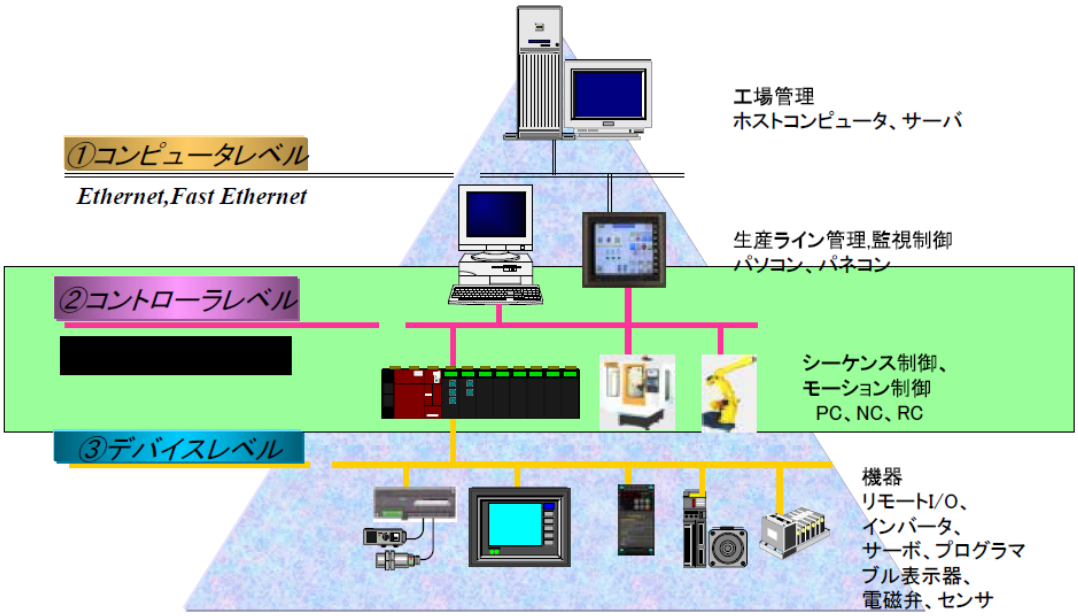

図 1

社団法人日本電機工業会　資料から作成

企業の情報システムにおいてはかつての中央集権型、シングルベンダーのホスト系システムであったものから、ネオダマ（ネットワーク、オープン化、ダウンサイジング、マルチメディア/マルチベンダー）と表現されたようなクライアントサーバー型、オープンでマルチベンダーのシステムへと急速に導入が進んだ。この背景には企業側のコスト削減志向と、同時にインターネットインフラの活用やシステムに対する柔軟性、システムの高度化への要求などユーザのニーズにも適うものであった。これらネットワーク化、オープン化等の利点は制御システムを利用する現場でも認められており、すでに挙げた点のほか管理容易性や設備投資軽減などさまざまなメリットがある。

制御システムのオープン化はすでに進展していることは「大規模プラント・ネットワークセキュリティ対策委員会」（１９９９、通商産業省 ）で指摘されており、その場合の脅威についても議論が行われている。また今後オープン化が進展する点も予想されている。

表 2

第 1 世代	1970 年代～1980 年代後半	・コンソール、コントローラともベンダ各社のOSを使用している。
		・制御システムと情報システムとの通信は、回線容量が小さく、1対1で接続されており、データ交換などの アプリケーション層の通信プロトコルはベンダ固有または接続の都度相互に決めて行われていた。
第 2 世代	1980 年代後半～ 1990 年代前半	・コンソールのOSは主にUNIX、コントローラはベンダ独自のOSを使用している。
		・Ethernet 接続は情報系LANや制御系情報LANの中 でもごく一部に限られており、パソコンのネットワークはまだ普及しておらず、社外へのインターネットなどとのオープンな接続もほとんどない。制御LANはベンダ固有の通信プロトコルを採用している。
		・UNIX系OSとTCP／IPプロトコルに精通した者であればコンソールまでの不正侵入は可能である。但しコントローラへのクラッキングは対象プラントの制御システムの構造を充分に知らないと不可能である。
第 3 世代	1990 年代後半	・コンソールのOSはUNIX系およびWindowsNT等の汎用OSを使用している。コントローラはベンダ独自のOSを使用している。
		・汎用OSのネットワーク技術を活用することにより、オープン化が進んでいる。
		・汎用OSのネットワーク技術に精通した者であれば、コンソールまでは比較的容易に侵入でき、パソコンを含む社内、社外のネットワーク接続の普及により、クラッキングの脅威が高まりつつある。

○制御システムの今後の傾向		
	全社レベルの情報システムとの接続	ERP(Enterprise Resource Planning) パッケージの適用、情報系既存システムとの情報共有、等
	プラントの情報システムとの接続、高度化、分散化、統合化	PIMS (Plant System) の適用 、 Information Management
	オープン化	汎用技術の採用(フィールドバス、TCP/IP)
	汎用化	専用OSから汎用OSへのシフト

「大規模プラント・ネットワークセキュリティ対策委員会」(1999、通商産業省)

6. 国内の制御システム用通信プロトコルの概況

6.1 ヒアリング結果

制御システムで利用されるプロトコルは、産業領域ごとに標準化されているもの、事実上標準となっているものも含め多くのプロトコルが存在する。今回の調査ではあらかじめ用意したプロトコルのリストの中から国内で利用者が多いと思われるプロトコルを列挙してもらった。下記は対象プロトコルの選別基準である。

１）「IP」、「TCP」、「UDP」などインターネットでも利用されるプロトコルを採用しているもの

２）仕様が標準化又は公開されているもの

３）制御システムにおいて、情報システムとの接続が考えられる、「コントローラレベル」又は「コントロールネットワーク層」で利用されるもの

４）国内で積極的に開発された又は普及が進められたもの

ヒアリングの結果、制御システムの通信プロトコルのうち、海外に比して日本国内の利用割合が高いと思われるプロトコルは「CC-Link」と「FL-net」（後述）であった。これらプロトコルは国内製品開発者が中心となって普及に努めており、日本や近隣アジア各国でも利用が進んでいる。

「FL-net」の適用分野が入手可能であったため、表３に記した。

表 3

加工組み立て産業

産業分野	設備名
自動車製造	エンジン機械加工ライン
	エンジン組み立てライン
	エンジン組み付けライン
	エンジン試験装置
	ボディー溶接ライン
	製造ラインの部品管理
	車両組み立てライン
半導体製造	半導体製造プロセス内(装置)
	バッチ式ウェハ洗浄装置
	エッチング装置
	液晶セル工程
表示デバイス製造	液晶製造ライン
	搬送システム
	液晶表示デバイス製造後工程
	液晶貼り合わせ装置
	ブラウン管製造ライン
	焼成炉
	基板位置決め設備
電気機器・電線製造	企業内の情報管理システム
	光ケーブル製造ライン
	太陽電池セル生産
	部品加工ライン
	整流器設備
機械製造	メカトロ製品製造設備
	部品加工ライン
	射出成形機

プロセス産業と食品・薬品産業

産業分野	設備名
製鉄・鉄鋼	鉄鋼製造ライン監視制御設備
	溶銑処理ライン
	精錬処理ライン
	圧延制御設備・搬送設備
	原料輸送ライン
	棒鋼圧延計量ライン
	受変電
紙パルプ	紙パルプ製造ライン監視制御設備
	抄紙機
化学	化学プラント運転制御
	薬液混合プラント
	タイヤ製造ライン
	洗剤製造設備
	プラスチック成形ライン
	メッキ処理装置
窯業	セメント製造キルン
	セメント製造搬送設備
	特殊ガラス製造の制御
石油	石油精製所動力設備

プロセス産業と食品・薬品産業

産業分野	設備名
食品	食品製造ライン運転制御
	液体充填機械
	飲料工場、ユーティリティ(空調)
薬品	薬品製造ライン運転制御
印刷	新聞印刷、出荷ライン
	ダンボール印刷後工程

公共・社会システム、その他

産業分野	設備名
公共・社会環境・防災設備	ダム／貯水池監視設備
	ダム管理システム
	ダム設備制御
	ゴミ処理計装設備
	ゴミ焼却場設備
	水門制御システム
	上下水道監視制御
	下水処理場
	浄水場
	下水浄化センタ、中継ポンプ場
	水処理中央監視盤
	排水機場
	水処理受変電
	ポンプ設備
	ポンプ場監視
	空港設備
	上水道テレメータ
電力	発電所運転制御
	電力変換器監視設備
	燃料電池監視制御設備
教育	大学構内設備、監視制御
ビル	ビル空調設備、監視制御
	コージェネ監視制御
	中央監視装置
	入退室管理
その他	ボイラ計装
	採石場の監視制御
	情報収集ネットワーク
	エネルギー使用量計測
	ゴルフ場散水設備
	仕分け装置

「FL-net（OPCN-2）2006 年度出荷実績調査報告」

（2007 年 6 月、JEMA ネットワーク推進特別委員会）

また、今後採用が進むプロトコルを考えるにあたって、変動要因となる項目として以下が挙げられた。

・ 欧米企業とのネットワークの共通化の進展
➢ 欧米企業との共通ネットワーク構築
➢ 外資企業の日本進出（生産拠点配置、M&A 等）
・ 設備投資サイクル要因
➢ 工場建設、拠点移動
・ 国内製品開発者の標準化に対する戦略の動向

6.2 プロトコル推進団体の確認

多くのオープンなプロトコルには非営利団体・ベンダ会・ユーザ会といった形で、普及啓発・ライセンスや技術情報の管理・相互運用性に関する情報提供、等のための組織が存在する。そのうち日本国内で支部などが設立されているものは、利用が進んでいるか又は普及に力がいれられていると思われるため、アンケートを行った（付随情報はホームページ又は公開資料より抽出)。

但し、アンケートを行ったところ、すべてのプロトコル推進団体から「国内で利用されているユーザ数は正確に把握していない」又は無回答であったため、欠測とした。

表 4

団体名	会員数	出荷数に関する指標（公開情報から）	プロトコル名	情報入手先
ＭＥＣＨＡＴＲＯＬＩＮＫ協会	264 社（2008 年 3 月、Worldwide）	出荷ノード数：60 万（Worldwide：通信ＡＳＩＣ総出荷ノード） 対応製品数：164	MECHATROLINK	http://www.mechatrolink.org/jp/index_jp.html
ＯＤＶＡ　日本支部	266 社（2007 年 11 月、Worldwide）	（記載見当たらず）	Common Industrial Protocol (CIP)	http://www.odva.org/
		（記載見当たらず）	ControlNet	
		（記載見当たらず）	DeviceNet	
		Ethernet/IP：70 万ノード以上（Worldwide）	Ethernet/IP	
ＣＣ－Ｌｉｎｋ　協会	853 社(2006 年末、海外 470：日本 383)	累積出荷ノード数：420 万 対応製品数（累積製品認可数）：838	CC-Link	http://www.cc-link.org/
EtherCAT　Technology　Group	760 社（2008 年 5 月、Worldwide）	（記載見当たらず）	EtherCAT（Ethernet for Control Automation Technology）	http://www.ethercat.org/
社団法人日本電機工業会	（記載見当たらず）	出荷実績：2 万 5000 ノード(2005 年) 認証機器：43	FL-net（OPCN-2）	http://www.jema-net.or.jp/

日本　ＡＳ－ｉ　協会	280 社（2008 年 5 月、世界）	（記載見当たらず）	Actuator-Sensor（AS）Interface	http://www.as-i.jp/
日本プロフィバス協会	1400 社以上（2008 年 4 月、日本 82 社）	累積出荷ノード数：2000 万 対応製品数：2500 以上	PROFIbus、PROFInet	http://www.profibus.jp/
NPO 法人日本フィールドバス協会	315 社以上（2008 年 4 月）	（記載見当たらず）	Foundation Fieldbus/H1 Foundation Fieldbus/HSE	http://www.fieldbus.org/index.php?option=com_content&task=view&id=172&Itemid=351
日本 OPC 協議会	451 社以上（2008 年 4 月、日本 48 社）	（記載見当たらず）	OPC OPC UA	http://www.opcjapan.org/

6.3 市場調査資料から

・　産業用 Ethernet 技術の進展

海外を中心に Ethernet 技術はオフィスにとどまらず制御システムでも利用が進みつつあり、標準規格として IEC/TC65/SC65C の WG11 と MT9 によって標準化作業が進められている。国内での実績は少ないが三菱電機「MelsecNetG」、オムロン「Ethernet/IP 対応 PLC ユニット販売」など販売が始まるなど、徐々に産業用 Ethernet の国内利用状況は変化していくと思われる。主なニーズとして大容量のデータ通信があり、「プロセスデータ管理」「遠隔監視・制御ニーズ」「フィールド機器のインテリジェンス化」の他、「無線 LAN」「海外からの影響」「(XML を利用した) 複数規格間の接続」といったニーズがある。(『産業用 Ethernet 関連機器の業種別ニーズ実態と市場展望』(2007 年 2 月、株式会社富士経済) より)

・　組込み機器向け通信機能へのニーズ

組込み製品向けの OS、ミドルウェア、の高機能化に伴いネットワークへの対応ニーズが高い。そのため、TCP/IP や IPSec/SSL、等の通信コンポーネント採用は徐々に広がりを見せている。組込み製品そのものは本調査のテーマとは離れるが、Windows や Linux などの汎用 OS 以外の領域でも標準化・規格化された通信プロトコルを採用した製品の利用が進んでいる点を留意しておきたい。(『エンベデッドシステムマーケット 2008』(2008 年 3 月、株式会社富士経済) より)

6.4 産業分野の観点からみた状況

・ビル・オートメーション分野

ビル・オートメーション分野のシステムは IP 化・標準化・オープン化が進んでおり、システムに採用されている通信プロトコルに関しても同様である。藤原憲明「ビルオートメーションシステムにおける統合ネットワーク」(2007 年、電気設備学会誌) によると、「ASHRAE」(米国暖房冷凍空調学会)、「BACnet」(米国標準規格) と「LonWorks」(エシュロン社) が主なプロトコルである。

・　リモート監視サービス

リモート監視サービスは公衆網、専用線、インターネットなどの通信網を利用し遠隔から監視を行うサービスである。市場は 2006 年に 9410 億円であり、今後も広がりを見せていくことが予想される。監視サービスの対象は家庭から電力設備まで多岐にわたる。海外を見ると効率性、高度な集中管理の必要性から石油パイプライン、天然ガス供給ラインなど重要インフラの地理的に離れたシステムの監視制御を行う場合にリモート監視制御を行う事例がある。下記の家庭向けや商業向けは本調査のテーマからはやや外れるが、監視サービスそのものは国内でも一般化されたサービスであるので国内での利用方法を示す意味で表 5 に監視サービスの分類を示す。

表 5

ビル向けリモート監視サービス	ビル総合リモート監視サービス
	空調設備リモート監視サービス
	エレベーターリモート監視サービス
	防犯・防災リモート監視サービス
	受変電設備リモート監視サービス
	コジェネシステムリモート監視サービス
商業向けリモート監視サービス	店舗向け本部システム ASP サービス
	商業店舗向けエネルギー監視サービス
	自動販売機リモート監視サービス
	駐車場リモート監視サービス
	冷凍・冷蔵ショーケースリモート監視サービス
工場・プラント・産業向けリモート監視サービス	工場・プラント向けリモート監視サービス
	養殖施設向けリモート監視サービス
	農業施設向けリモート監視サービス
	物流拠点リモート監視サービス
家庭向けリモート監視サービス	家電制御リモート監視サービス
	ホームエネルギーマネージメントサービス
	防犯・防災リモート監視サービス
	カメラ系リモート監視サービス
	高齢者安否確認サービス
	在宅健康管理システム
	LP ガスリモート監視サービス
	都市ガスリモート監視サービス
インフラ向けリモート監視サービス	マンホールポンプ場リモート監視サービス
	道路状況リモート監視サービス
	流域管理リモート監視サービス
	工事現場リモート監視サービス

「リモート監視関連市場徹底総調査」（2007、富士経済）より作成

○その他国内の動向がわかる活動など

国内の関連セミナー、ワークショップ、シンポジウム(オープンなもの)

- JEITA　産業社会制御システムフォーラム
- Manufacturing Open Forum (MOF)
- SICE Annual Conference

・ 重要インフラ情報セキュリティセミナー　（一般社団法人 JPCERT コーディネーションセンター、独立行政法人情報処理推進機構　共催）

備考：

「FL-net」について

1996 年 4 月に（社）日本自動車工業会(JAMA)は、通産省を通じて（財）製造科学技術センター（MSTC）に対して“ＦＡネットワーク要件書”を提案した。（財）製造科学技術センターではこれを受けＦＡオープン推進協議会（JOP）内ＦＡコントロールネットワーク専門委員会を設置し、要求仕様の検討、既存ネットワーク技術の調査を行い、基本仕様を策定し、その後実証・適合性試験方法など必要な開発を進め完成した。2000 年より（社）日本電機工業会に移管され、規格・認証・普及促進業務が行われている。FL-net は当初より FA ネットワーク化、オープン化、マルチベンダーを実現することを目指し、情報システムとの連携や調達コストダウンの観点からイーサネットを採用することで検討されていた。

「CC-Link」について

三菱電機が 1996 年に発表したフィールドバス。CC-Link は FA における 3 階層の階層型ネットワークアーキテクチャにおいて、フィールド機器（リモート I/O、アナログ I/O、インバータ、表示機など）とパソコン・PLC 等のコントローラ機器とを接続するフィールドネットワークに属する。（2006 年 10 月　月刊計装 Vol.49）

7. 国内の制御システムセキュリティに関する取り組み活動の概況

7.1 制御システムセキュリティについて研究活動を行っている国内の主要な団体

- JEITA[7](社団法人 電子情報技術産業協会)制御システム専門委員会セキュリティWG
- JEMIMA[8](日本電気計測器工業会)セキュリティ調査・研究WG
- SICE[9]（社団法人 計測自動制御学会）計測・ネットワーク部会

上記団体は相互に協力がなされ協働して成果発表を行っている。

なお、上記の団体とは別に、電力システム分野においては電力中央研究所が研究活動を進めている。

過去に、「大規模プラント・ネットワークセキュリティ対策委員会」（１９９７、通商産業省[10]）においてサイバーテロ対策の観点から制御システムセキュリティも含めたプラントシステム全体のセキュリティ対策について幅広に議論がなされた。適用領域が幅広く、かつ時間的な制約で多くは課題抽出に時間が費やされた内容となっている。本調査では今後の施策を検討するために活動概要と課題のみを引用し取り上げたい（最終報告書は独立行政法人情報処理推進機構Webサイトで公開され入手可能である)。

■大規模プラント・ネットワークセキュリティ対策委員会設立の背景：

「本委員会の背景は、中間報告書の６ページにおいて、以下の通り説明されている。

「近年の情報化の進展に伴い、経済・社会の多くの分野が業務の効率性、生産性の向上などのため、コンピュータ・ネットワーク・システムに依存するようになってきている。その結果、コンピュータ・ネットワーク・システムの機能が停止したり不完全になると、経済活動はもとより、国民生活全般に深刻な影響を及ぼすことになる。

いわゆるサイバーテロリズムなどの脅威に対し充分なセキュリティ対策をとることが、これからの高度情報通信社会の構築に不可欠である。

プラントのコンピュータ・ネットワーク・システムを構成している情報システムと制御システムは、単体の独立したコンピュータから専用線や専用プロトコルを用いた閉域接続のネットワークへ、さらには標準プロトコルを用いた開放型システム間相互接続へと発展してきている。

情報システムのネットワーク・セキュリティ対策に関しては「コンピュータ不正

7 http://www.jeita.or.jp/japanese/
8 http://www.jemima.or.jp/
9 http://www.sice.or.jp/
10 http://www.ipa.go.jp/security/fy11/report/contents/intrusion/psec/index3.html

アクセス対策基準解説書」（1996.11.15）等がすでに存在するので、本委員会では制御システムを主対象として、クラッキングを主としたネットワーク・セキュリティ対策を検討した。」

■想定する主な脅威：

「クラッキング」

「サイバーテロリズム」

■委員会運営等：

3 つの分科会とワーキンググループ

「ユーザ企業分科会」

「エンジニアリング企業分科会」

「ベンダ企業分科会」

■活動の概要：

4 つの提言（中間報告）

「プラント用セキュリティ・ガイドラインの策定」

「ネットワーク・セキュリティにおける脅威分析手法の実証」

「防止技術の研究開発」

「ネットワーク・セキュリティに関する普及啓発」

6 つの検討課題（中間報告後、最終報告まで）

<非技術的事項>

①「セキュリティ・マネージメントの研究」

②「セキュリティ運用ガイドラインの策定」

③「国際会議」

<技術的事項>

④「防止技術の研究開発の企画」

⑤「リスク分析手法の研究開発の企画」

⑥「セキュリティ評価基準の策定」

■今後の課題など

①「セキュリティ・マネージメントの研究」

- 専門家の不足
- コミュニケーションギャップ

「IT 担当者と経営者を含めた他部門との間に存在すると考えられる。（中略）セキュリティ対策は端末機器に接触する全ての人々が理解し、実行しなくてはならないものであり、またトップ・マネージメントの主要な責務であるリスク・マネージメントを行ううえでも、コンピュータ・ネットワークのリスクを十分把握する必要がある。（中略）大切なことは、自動車の安全運転の履行を促すことであり、

エアーバッグや ABS 装置の構造の説明ではない。」

②「セキュリティ運用ガイドラインの策定」

- 「運用ガイドラインの適用方法を示す解説書を作成することを今後の課題として提示する。」

④「防止技術の研究開発の企画」

- 「今後は更に、DCS に限定せず制御システム全体としてのセキュリティ機能の検討、セキュリティ機能の全体の統合化、実装を前提とした再検討などを考慮した、製品化に向けた設計が必要であり、来年度以降の課題として残されている。」

⑤「リスク分析手法の研究開発の企画」

- プラント・セキュリティ・エンジニアリング
- 「プラント・エンジニアリングは、基本設計から詳細設計へと各設計の段階に応じた系統的な設計手法とリスク分析手法がすでに確立され、プラント・エンジニアリングに対するセーフティ・エンジニアリングの位置づけが確立している。
  これに対し、ネットワーク・エンジニアリングは、基本設計、詳細設計の流れの中で系統化されたネットワークの設計手法が今のところ定まっていないように思われる。このことが、セキュリティ・エンジニアリングのためにネットワーク用リスク分析手法を系統化して纏めていくうえでネックになる可能性がある。したがって、基本設計、詳細設計の流れの中で系統化されたネットワークの設計手法が必要である。」
- プラントネットワークに対するリスク分析
- その他
- 実証試験システムの開発の必要性
- リスク回避手段の最適投入に関する指針の策定
- セキュリティ・ポリシーに対する人的要因に関するリスク分析
- FTA 用確率情報の収集

⑥「セキュリティ評価基準の策定」

- システムを対象とする PP を記述することに内在する課題
- PP 記述形式上の課題
- 個別機器の PP 検討への発展可能性

「TOE の確定作業において、我々は制御システム部分の全体を対象とした。この中で、各機器、コンポーネントの位置づけ、そのセキュリティ機能要件が明確になってきたものとして、以下に例示する。

<プロセス・コンピュータの位置づけ>

「情報システム」側からの情報要求に応える機能を持つ装置として位置づけることができる。同時に「情報システム」側からのセキュリティ侵害の経路となりう

る装置ともいえる。「制御システム」全体を境界において守るのに必要なセキュリティ機能が実装される装置として期待される。

<コンソール>

経営管理組織の該当部門の権限管理機構をシステム的に反映しうる権限管理機能の必要性が求められる。権限管理の対象となるシステム上の資源は「コントローラ」に限らず、今回のセキュリティ境界内にある「プロセス・コンピュータ」や「RAS」も対象となるはずである。

このような位置づけを前提に、個別の PP を策定していくのは有意義であると考える。」

「全体的な視点からの課題」

- 「セキュリティに対する理解を啓発する活動」

  「啓発活動では、対象者を特定化する工夫（たとえば、企業経営者、技術者など重層的に特化する）が必要である。また、平成１１年の情報化月間に開催したシンポジウムと同様の機会を継続して設けるなど社会的課題としての位置付けることも重要である。」

- 「セキュリティ問題を継続的に取扱う機関の設置」

  「本委員会は期間限定で活動してきたが、今後の技術進歩や海外の動向などについて継続的に関心を持ち、調査、公表などを行うことが必要である。特に、継続的な国際交流は不可欠であり、ボーダレスな環境を考えると我が国の関係者の交流がなければ、セキュリティについての十分な対応が不可能である。専門家育成や対策研究などの役割を含めて、専門機関を常設することが必要である。」

- 「実証的な横展開の活動」

  「本委員会はプラント・ネットワークを対象として調査研究したが、その成果を個別のプラント・ネットワークに当てはめて行う実証的な事例研究が必要である。問題の性質上、個別の研究内容の大部分は非公開となるが、本委員会の成果に対する評価部分が公開されれば有用である。」

  また、本委員会と同様の活動が、他産業においても展開されることが必要である。

- 「その他」

  「プラント・ネットワークのセキュリティ分析手法などの技術開発に関する研究課題、セキュリティ評価の定量化などの理論面の研究課題、およびプラントの運用におけるセキュリティレベルの向上、必要な改善策についての研究課題など多数残されている。詳細はＷＧ活動報告を参照していただきたい。」

8. まとめ

今回の調査を通じて、国内の制御システムのセキュリティに関する現状について、以下のような知見を得ることができた。

- 制御システムは、極めて多様であって、利用している業界や納入ベンダに依存して異なる方式や技術が採用されている。そのため情報が分散しており、全体概要を捉えることが容易でない。
- 制御システムの中で利用される通信プロトコルは、利用分野ごとに異なっており、標準化が進んでいる IT 系システムと比較して、全体として極めて種類が多い。したがって、制御システム用の通信プロトコルに関連する脆弱性情報の取扱いにあたっては、当該プロトコルを利用している業界を理解した上で、影響の推定や対応方法の判断を行うことが重要である。
- IT 系システムと同様のオープン・システムの採用やマルチベンダー化を通じて，コストダウンを求める圧力が強い応用領域を中心に、ビル・オートメーションの領域など制御システムにおいても、標準化された通信プロトコルやイーサネット技術、汎用 OS などの採用が進み始めている。
- 国内の制御システムのベンダも含めて、各社の制御システム用プロトコルの国際標準規格化や、その普及推進に努力が払われており、各種の推進団体が作られている。しかしながら、ほとんどの推進団体は、ライセンスや技術情報の提供など活動を行っているのみで、「利用実態については把握していない」模様である。
- 制御システムを提供している主要国内ベンダは、顧客への説明その他の理由から、セキュリティ問題に関心を持ち始めており、業界団体や学術学会の下に研究会を設けて、勉強会の実施や情報交換を進めている。
- 国際標準の通信プロトコルの国内での利用や、日本発で国際標準となっている通信プロトコルの海外利用が広がりを見せ始めている。したがって、CERT/CC をはじめとする海外の脆弱性調整機関との連携も今後一層重要性を増すものと見込まれる。

  大規模プラント・ネットワークのセキュリティについては、1997 年に通商産業(当時)の主導で大規模な調査が行われ、調査結果の報告書が公表されている。この調査から 10 年が経過しているが、結果が公表された、これに匹敵する規模の大規模調査はその後は実施されていない。

  以上のような調査結果にかんがみ、脆弱性情報やインシデントに関する調整機関としての JPCERT/CC には、今後以下のような活動を強化推進することが求められているといえよう。
- 制御システムのベンダ各社の POC(Point of Contact)の拡充
- 制御システムを提供しているベンダや利用組織のコミュニティにおいて進められるセキュリティ関連活動に資するような情報の提供などの、セキュリティ専門機関としての

支援

- 利用分野別の制御システムのセキュリティへの取組み状況の把握
- 対策情報の開示方法を中心とする、制御システムの脆弱性情報取扱いの在り方に関する検討
- 重大な脆弱性が明らかとなった場合や，インシデント発生時に備えた、制御システム関係者との円滑な連携を可能とする枠組みづくり

【補足】

「一般社団法人　JPCERT　コーディネーションセンター」

インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、技術的な立場から、特定の政府機関や企業からは独立した中立の組織として、日本における情報セキュリティ対策活動の向上に取り組んでいる。脆弱性情報においては早期警戒パートナーシップ [11]に基づいて調整機関として製品開発者との調整と利用者への周知を目的としてその情報の公開を行っている。

https://www.jpcert.or.jp/

「情報セキュリティ早期警戒パートナーシップガイドライン」

「情報セキュリティ早期警戒パートナーシップ」は、「ソフトウエア等脆弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）の告示を踏まえ、国内におけるソフトウエア等の脆弱性関連情報を適切に流通させるために作られた枠組みです。

IPA、JPCERT/CC、社団法人 電子情報技術産業協会(略称：JEITA)、社団法人コンピュータソフトウェア協会(略称：CSAJ)、社団法人 情報サービス産業協会(略称：JISA)及び特定非営利活動法人日本ネットワーク・セキュリティ協会(略称：JNSA)は、脆弱性関連情報の適切な流通により、コンピュータウイルス、不正アクセスなどによる被害発生を抑制するために、関係者及び関係業界と協調して国内におけるソフトウエア等の脆弱性関連情報を適切に取り扱うための指針「情報セキュリティ早期警戒パートナーシップガイドライン」を策定、運用しています。

http://www.ipa.go.jp/security/ciadr/partnership_guide.html

「オープン規格の通信プロトコル」

代表的なプロトコルである TCP/IP を例に取ると、すでに研究者などにより複数の脆弱性が発見・公開されています。独立行政法人 情報処理推進機構セキュリティセンター「TCP/IP に係る既知の脆弱性に関する調査報告書 改訂第 3 版」に 23 の脆弱性情報の詳細がまとめられています。

http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

[11] http://www.jpcert.or.jp/vh/

【参考文献・資料入手元】

1) 『ソフトウエア等脆弱性関連情報取扱基準』(平成 16 年経済産業省告示 第２３５号)
http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf
2) 「大規模プラント・ネットワークセキュリティ対策委員会」(１９９９、通商産業省)
http://www.ipa.go.jp/security/fy11/report/contents/intrusion/psec/index3.html
3) 『電気設備学会誌』Vol.27 特集：監視装置の動向・インターフェース技術（2007 年 12 月、社団法人電気設備学会）
4) 『産業用 Ethernet 関連機器の業種別ニーズ実態と市場展望』(2007 年 2 月、株式会社富士経済)
5) 『エンベデッドシステムマーケット 2008』(2008 年 3 月、株式会社富士経済)
6) 『ビルオートメーションシステムにおける IP 化・オープン化関連市場実態調査』(2007 年 9 月、株式会社富士経済)
7) 『2007 リモート監視関連市場徹底総調査』(2007 年 7 月、株式会社富士経済)
8) 『月刊計装』各号、工業技術社
9) 『NIST SP 800-82 DRAFT Guide to Industrial Control Systems (ICS) Security"』
http://csrc.nist.gov/publications/PubsDrafts.html
10) 「Manufacturing Open Forum 2008 (MOF2008)」(主催：IA 懇談会、協賛：VEC、参加団体：MfgX 他 15 団体)
http://www.mstc.or.jp/mfgx/
11) 「ビル管理の世界でも進むオープン化、IPv6 組み合わせた相互接続デモを実施」(Interop2005)
http://www.itmedia.co.jp/enterprise/articles/0506/09/news012.html
12) ・重要インフラ情報セキュリティフォーラム 2008 ～重要インフラ関係者の情報共有～（独立行政法人情報処理推進機構（IPA)、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）共催）
http://www.ipa.go.jp/security/event/2007/infra-sem/
13) 第二回産業社会制御システムフォーラム（社団法人 電子情報技術産業協会（JEITA）主催）
http://www.jesa.or.jp/csf/
14) SICE Annual Conference 2008 (社団法人 計測自動制御学会(SICE)
http://www.sice.or.jp/sice2008/

【調査資料】

表 6　制御システムプロトコルリスト

番号	プロトコル名称	情報入手先
1	Foundation Fieldbus/H1	http://www.fieldbus.org/
2	Foundation Fieldbus/HSE	http://www.fieldbus.org/
3	INTERBUS	http://pl.et.fh-duesseldorf.de/prak/prake/download/IBS_grundlagen.pdf
4	Modbus	http://www.modbus.org/
5	Modbus Plus	http://www.modbus.org/
6	Modbus TCP	http://www.modbus.org/
7	Profibus	http://www.profibus.com/
8	Profinet	http://www.profibus.com/
9	Common Industrial Protocol (CIP)	http://www.odva.org/
10	ControlNet	http://www.odva.org/
11	DeviceNet	http://www.odva.org/
12	Ethernet/IP	http://www.odva.org/
13	MECHATROLINK	http://www.mechatrolink.org/
14	Omron FINs	http://www.omron.com
15	Actuator-Sensor (AS) Interface	http://www.as-interface.net/
16	ARCNET	http://www.arcnet.com
17	Controller Area Network (CAN)	http://www.can-cia.org/
18	CANopen	http://www.can-cia.org/
19	MELSECNET/H or /10	http://www.mitsubishi-automation.com/products/networks_melsecnet10h.html
20	CC-Link	http://www.cc-linkamerica.org/ http://www.cc-link.org/jp/
21	SERCOS	http://www.sercos.com
22	TCnet (Time-critical Control Network)	http://www3.toshiba.co.jp/sic/english/seigyo/tcnet/index.htm
23	GE Service Request Transfer Protocol (SRTP)	http://www.gefanuc.com/

24	HART (Highway Addressable Remote Transducer)	http://www.hartcomm2.org/
25	NetDDE, FastDDE	http://www.wonderware.com/
26	SINEC-H	http://w1.siemens.com/
27	Vnet/IP	http://www.yokogawa.com/
28	EtherCAT (Ethernet for Control Automation Technology)	http://www.ethercat.org/
29	OPC	http://www.opcfoundation.org/
30	OPC UA	http://www.opcfoundation.org/
	JDDAC	http://jddac.dev.java.net/
31	ICCP/TASE.2, IEC 60870-6	http://www.iec.ch/
32	IEC 60870-5 (101, 102, 103, 104)	http://www.iec.ch/
33	IEC 61850	http://www.iec.ch/
34	IEC 62351	http://www.iec.ch/
35	DNP3	http://www.dnp.org/
36	CIM / IEC 61970 and 61968	http://www.iec.ch/
37	UCA 2.0	http://www.epri.com/
38	OpenAMI	http://osgug.ucaiug.org/sgsystems/OpenAMIEnt/default.aspx
39	Manufacturing Message Specification (MMS) ISO 9506	http://www.iec.ch/
40	BACnet (ISO/IEC 16484-5)	http://www.bacnet.org/
41	BACnet/IP	http://www.bacnet.org/
42	KNXnet/IP	http://www.knx.org/
43	LonTalk (Echelon) EIA-790.1	http://www.lonmark.org/