生産システムと周辺のセキュリティを考える
制御システムの構造から見る、セキュリティの適所適性対処について

VEC 事務局　村上正志

１．はじめに

製造業におけるシステムとしては、生産システムと制御システムとに区別して考えることができる。
制御システムにインターネット接続することまで考えていなかった時は、「ありえない。」「不要だ。」と言っていたが、今は、IT の導入によって利便性を追求してきたことで、リスクの重みを意識しないでここまできている節があるように感じられる。
ユーザ、システムエンジニア、装置ベンダとしては、リスクを的確に捉えて、その対策を講じることが求められるのではないだろうか。そのためにも、製造する製品の特徴や生産方式によって条件が異なる生産現場の生産システムで制御システムそのものの構造により、セキュリティがどの程度必要なのかを考え、定義し、どのような対策を取るべきかの指針をまとめておく必要があると思う。
本件では、その作成に当たり参考となる情報を挙げてみた。

２．ハザード事例

2009 年 2 月 18 日と 19 日に、経済産業省情報セキュリティ政策局と JPCERT 主催の制御システムセキュリティワークショップとカンファレンスが開催された。
その中で、海外における工場や発電所や公共施設などで、どのようなテロ行為の事故が発生してきているかを紹介された。原子力発電所へのテロ攻撃や交通システムへのテロ事件も紹介された。高校生が工場の排水設備を攻撃して汚水が川に流れて大ダメージを与えた事件もあった。C 言語を勉強して、ブラックマーケット Web サイトで販売されているツールを使うと数十分で企業のネットワークに攻撃できるというデモもあった。
特に、アイダホ国立研究所のマーティ・エドワーズ氏が発表された実験結果が衝撃的であった。それは、工場側を想定して実機プラントの制御システムセキュリティを組むチームとそれを攻撃するチームにエンジニアが分かれて戦うというものだが、開始して１０分程度で、実機プラントの液体はバルブから溢れ出し、異常発生となったが監視制御システムの DCS 画面には警報も出なければ、停止もしないで正常状態で動いている為、オペレータは異常事故が起きていることさえ知ることができなかったということを実際に撮影したビデオを見せて紹介された。

国内において起きているハザード事例としては、工場の設備の改善工事で入ってきた作業者の PC からビールスが制御システムに侵入して、生産そのものができなくなったというものだ。汚染された制御システムを元に戻す作業は、検証テストも含め、一週間程度かかって、やっと生産稼働できたという情報もある。一週間程生産ができなかったこととその復帰作業にかかった費用を考えると企業としては、かなりのダメージである。その原因は、サービス作業者の PC を個人的なことに使用していたことによりインターネットでのビールスを引き込んでしまったことによるという。

これらの事例は、業務上の PC と生産システム／制御システムの PC のネットワークを分けているからといっても、ハザードは存在することを教えてくれる。

２．制御システムセキュリティにおける危険度

製造現場での制御システムでは、生産する製品により生産方式が異なっている。それにより、大きく PA・FA・装置と分けてみることができる。

１）PA 制御システムにおける危険度について

従来、DDC（Direct Digital-Control System）での制御システム制御盤と検出端（温度センサーや圧力トランスミッター／流量トランスミッター／ポジション・トランスミッターなど）と操作端（圧力調節弁、流量調節弁、ダンパー開閉・ドライブ、アクチュエータ、I/P ポジショナーなど）との間では、４～２０mA／０～１００%、－１０ｖ～＋１０ｖ／０～１００%の信号で、アイソレート仕様で、２Φの２芯シールドケーブルで取り合いしている。操作員は、インジケータとスイッチ／ランプを組み合わせたメカニックな操作ステーションや CRT チューブもしくは液晶ディ

スプレイの画面とマイクロスイッチの上にシートを張った操作ステーションを使って操作端のポジションや制御偏差を見ながら手動操作（設定値変更や操作端の開閉操作など）を行ったり、自動／手動切り替え操作を行い、運転監視をするが、その操作ステーションと制御システムのコントローラとの間は、専用のケーブルで専用のプロトコル仕様での通信を行っている。
制御システムは、コントローラモジュールと I/O スレーブモジュールの構成が基本でその間は制御盤の中で専用バス通信でつながっている。
DCS（Distributed Control System）では、監視操作ステーションが専用のコンピュータを使用して、プラントの配管系統図や制御対象の状態図をディスプレイに表示し、リアルなデータを数値表示やアニメーション表示で状態を表現し、プロセス制御の監視画面を構成している。この監視操作ステーションが専用コンピュータでコントローラと接続しているデータ取り合いに OPC を採用しているベンダ製品も多い。
制御システム制御盤と検出端や操作端などのデバイス間をフィールドバスなど国際標準仕様の通信で接続している場合でも、シールドされた通信ケーブルを使用している。
また、複数のプラント制御で相互情報交換を行う場合は、プラントケーブルと呼ばれる専用通信を採用しており、ループケーブルを採用し、冗長化の為に二重にループケーブルを布くこともある。
ここまでの範囲でクローズしているプラントの制御システムでのセキュリティは、ベンダやエンジニアリング会社のエンジニアが PC を持ち込んで、制御コンフィグレーション入れ替え作業やチューニング作業をする際に、プラント制御に支障となるビールスを混入させることが考えられる。
また、運転員による自主保全や現場作業の効率化を図って、携帯 PDA に監視画面を表示し、検出端や操作端のチューニング操作で監視室の画面でのポジション確認を行うことができるが、その通信は無線通信やイントラネットやインターネットのいずれかを使用することになる。その場合、外部からの進入が可能となるので、ここにはセキュリティ対策が必要と考えられる。

DCS 製品の中には、SCADA ベンダの OEM を受けて、Windows 系の DCS を製品販売しているところもあり、この場合、SCADA ベンダからのセキュリティ対策情報公開に関する基本契約（Audit）は重要となろう。

２）FA 制御システムにおける危険度について
PLC やマイクロコントローラに、I/O デバイスを接続して制御を行う FA 制御システムでは、制御データをパソコンに取り込んで、Office アプリケーションツールを使って、生産管理業務をすることが広がっており、この場合のビールス進入の危険度は、考えられる。
また、監視用に SCADA を使用することも多く、SCADA の情報を業務用 PC に接続して、生産情報、生産製品の品質情報、設備の稼動情報などを取り込んで、使用している。この場合の接続されているもしくは間接的に関与している PC の健康状態も危険度有りと考えられる。
制御ネットワークのラインで一部無線通信を使用している場合、公開されていない専用プロトコルの通信仕様では、外部からの進入の可能性は低いだろうが、OA で使用している無線 LAN を使用している場合は、外部からの進入の可能性は高くなる。

３）装置の制御システムにおける危険度について
装置の中の制御システムにおける危険度は、コンフィギュレーション入れ替え作業やチューニング作業時に接続する PC から進入することが考えられる。
装置の外で、ユーザが情報収集・監視・管理の為にネットワーク接続する場合、Ethernet を使用することが多く、それに接続されている PC からの進入が考えられる。
また、無線通信を使用して、装置の遠隔監視操作を機能的に持つ装置も、外部からの進入が考えられる。
電話回線を使用したり、インターネットを使用して、装置の面倒をサービス会社もしくはベンダ／メーカに依頼している装置も外部からの進入の危険性があると考えられる。

３．生産システムセキュリティにおける危険度
制御システムで生産する製品の生産管理を担当する生産システムは、生産計画から生産指示、生産履歴、SCM、品質管理、設備管理、保全管理、など生産に関わる業務のシステムとして存在する。
１）生産管理系システムにおける危険度について

生産計画、生産スケジュール、SCM（Supply Chain Management）、生産指示・監視システムなどでは、社内 LAN を使用していることが多い。スタンダロンで使用していても USB メモリや CF カードなどで指示データを授受したり、生産実績情報を授受したりしている場合もある。これらの PC の健康状態は、監視範囲に入ることになる。

２）目的別 MES における危険度について
生産プロセスの実績記録（PIMS）を必ず行わなければならない業界や業種が増えてきている。医薬品医療品業界ではGMP、食品製造および食品加工製造業界ではHACCP、半導体製造業業界ではSEMI、電機組立て業界でもRoHS、ROCH、自動車業界ではコール対策で、というように、法規制や業界標準などの事情で、トレーサビリティを要求することが多くなっている。さらに、品質管理情報のリアル化、制御効率改善、設備保全のムダ削減管理、改善課題の調査や対策後の評価などの事情で、Historical Trend データを使用すること（LIMS）が多くなっている。
これに関わる PC やデバイスへ外部から進入する危険性があると考えられる。

３）業務で使用している PC における危険性について
会社の PC を使用して、休憩時間に個人的インターネットアクセスをして、業務に不要なアプリケーションやミュージックデータをダウンロードしたり、趣味のサイトを観たり、自宅から持ってきた音楽を入れて、聞いたり、お気に入りのビデオを見たりと、インターネットを使っていると危険度はかなり高くなると考えられる。
ノートパソコンを自宅に持って帰って、インターネットを使用していると、ファイヤ・ウォールのある無しで、さらに危険度は高まってくる。
また、個人所有の PC を会社に持ってきて、ネットワークに接続して、インターネット接続するのも危険度は、高くなる。

４）マイクロソフト社 Windows 系でのセキュリティ
Windows OS はオープン OS ではない。デファクト OS である。WindowsＸＰのセキュリティレベルは、かなり高いが、WindowsＮＴや Windows2000 が一台でもネットワーク上に存在するとセキュリティレベルは、ＮＴや 2000 レベルの極度に低いセキュリティレベルとなってしまう。だから、ＰＣを入れ替える時は全てＸＰとすることが良い。
また、制御系で使用しているＯＰＣなどでは、ＤＣＯＭを使用している。このＤＣＯＭは、ＸＰのＤＣＯＭのセキュリティレベルは高く、ＮＴや 2000 のＤＣＯＭのセキュリティは極度に低い。ＤＣＯＭそのものは、オープンなインターフェースなので、ガードができなければ監視することが必要と考える。

５）Linux は大丈夫という人がいるが、オープンソースということは、ソフトエンジニアであれば誰でも中の構造を知ることができるということになり、構造を知っていれば、進入し破壊することは容易であるということになる。そういう視点から対策を打っていくことが大切である。

３．ハザード分類
生産システム／制御システムセキュリティという課題を抱えて、いろいろ調べてみた。その範囲で以下わかったことを書き出してみる。
３．１　攻撃対象
攻撃対象としては、ネットワーク接続の PC のデータ取り合いを阻止したり、サーバの機能停止を目的としたり、クライアントからのアクセスを妨害したり、ハードウェアのファームウェアそのものに進入して操作進入をしたり、生産記録を盗んだり書き換えたりするなど、多様である。

３．２　現象の特徴
現象のタイプにもいろいろある。
ナパーム爆弾のように関連対象が一斉に異常となるタイプ
クラスター爆弾のように次々と連鎖的に転移して異常となるタイプ
人知れず異常を誘引するように仕掛けを忍ばせる工作員タイプ
などがある。

３．３　攻撃の分類

主要な攻撃の分類は、以下に挙げる。

１）外部からの攻撃手口

ﾌｨｯｼﾝｸﾞ：誘導メールを送りつけて仕掛けを施したWebサイトに誘い込むタイプ

本物に似せて作ったWebサイトに相手が引っかかってくるのを待つタイプ

SQLｲﾝｼﾞｪｸｼｮﾝ：SQLサーバを使用していることを想定して、想定外のSQL文実行操作でデータベース内の情報を搾取

Man Machine Interface in The Middle：正規のオペレータとサーバ間に割り込み不正アクセスを行う

ｸﾛｽｻｲﾄｽｸﾘﾌﾟﾃｨﾝｸﾞ：Webアクセス上の脆弱性を突いて、悪意のあるアプリケーションを侵入させる

２）故意過失による脅威

①不適切な行為

個人ｱｸｾｽ：社内のPCで個人興味のサイトへアクセス

個人のPCを持ち込んでネットワークに接続

②人為的ミス

PCや携帯PDAや携帯電話の紛失⇒情報漏洩、アクセス情報漏洩

USBﾒﾓﾘの紛失⇒情報漏洩

P2Pｿﾌﾄによるﾃﾞｰﾀ流出⇒情報漏洩

③悪意のある不正行為

ID／ﾊﾟｽﾜｰﾄﾞの盗用⇒攻撃手口搾取、犯罪手口供与

ID不正利用⇒アクセス権限不正使用、冤罪行為

データ書き換え⇒生産情報の書き換え、制御システムの制御ファイルの書き換え、生産レシピの書き換えなど

ﾊｰﾄﾞや媒体の持ち出し⇒情報横流し販売、産業スパイ行為

④感染

ｳｨﾙｽ／ﾜｰﾑ

ｽﾊﾟｲｳｪｱ／ｷｰﾛｶﾞｰ

ﾎﾞｯﾄﾈｯﾄ

３．４　攻撃対象は、Windows系OSだけではない。

セキュリティと言うとWindows系PCとサーバが攻撃される。それ以外は対象外。と思われるが、それは間違いである。LinuxもUnixもオラクルも対象である。また、特定のアプリケーションをターゲットにした攻撃もある。

C言語を知っている高校生が、闇マーケットで入手したテロツールを使って、企業サーバ攻撃をして、工場の排水に汚染物を出したことで川が汚染された事件も海外では起きている。

アイダホ国立研究所で行った実験で、工場を守る側と攻撃する側とに技術者を分けて紅白戦を行った。工場側は実際のプラント計装のシステムにセキュリティ対策を施した設備を使用した。

開始10分も立たないうちに、タンクからは液体が溢れ、バルブは半開きで停まる。しかし、DCSの画面にはタンクの液体が溢れた警報も出ないし、バルブも正常動作を示す表示のままであった。このビデオを2009年2月18日のJPCERTと経済産業省情報セキュリティ政策局共催の「制御システムセキュリティワークショップ」でアメリカ合衆国アイダホ国立研究所のマーティ・エドワーズ氏が日本で公開した。

つまり、Windows系OSのPCだけをセキュリティ強化すれば良いと言う考えは捨てるべきである。

４．生産システム／制御システムセキュリティ対策

生産システムにおけるセキュリティをどう対処するべきかの検討は、2006年から始まっている MOF（Manufacturing Open Forum：IA懇談会主催：財団法人製造科学技術センターが事務局を担当）やVEC（Virtual Engineering Company & Virtual End-User Community：VEC事務局）などで取り上げて検討し、セミナーなどで発表活動をしている。また、経済産業省情報セキュリティ政策局と JPCERT が主催する「制御システムセキュリティ・ワークショップ及びカンファレンス」（2009年2月18日19日開催）でも取り上げている。

参考となる資料が存在するWebサイト

MOF2008でのXMLコンソーシアム　セキュリティ部会検討報告

（ http://www.xmlconsortium.org/public_doc/mof2008_security/mof2008.html ）

まず、一般業務管理を行っているネットワークと生産システムとのネットワークを区別することから、考えて頂きたい。
さらに、生産そのものを実行している制御システムのネットワークをも区別して考えて頂きたい。
一般業務管理のネットワークに接続されている PC やサーバは、通常の情報系セキュリティ対策を施すことは言うまでも無いことである。
一般業務管理のPCはインターネット接続ができても、生産システムのネットワークに接続しているPCやサーバは、インターネット接続をしないことが望ましい。本社と工場間やロジックセンターと工場間の通信はセキュリティ保障された専用線を使用するとか、VPN 通信などを利用してセキュリティレベルを確保することをお勧めする。

制御システムネットワークに接続された PC には、リアルデータを扱う為にビールスバスタを仕掛けることができない。そこで、制御システムネットワークは、無菌室に相当する位置付けとなる。となれば、出入りするデータに雑菌やビールスがついていない管理をしなければならない。
制御システムのネットワークと生産業務管理のネットワークの間には、限定されたコマンドや情報アクセスだけを通過させるゲートウェイをお勧めする。
また、無線通信を制御システムに使用する場合は、一般業務で使用する無線通信とつながらない配慮が必要であり、無線通信搾取や妨害がされない環境を確保することが必要となる。

５．制御システムにおけるセキュリティ対策はどこまで考えるべきか
制御システムを守る基本は、
①侵入を防ぐ：ファイヤ・ウォール、ゲートウェイ、ルータ
②破壊されない：攻撃コード検知、無視、廃棄
③解読できない：暗号化
④改竄されない：パスワード
になるが、全てを実施するかどうかは、制御システムの構造とハザード性による。
そのセキュリティ対策ではベンダだからできることと、エンジニア会社だからできること、ユーザだからできることがある。

１）ベンダ／メーカの役割り
ベンダ／メーカとしての役割りとしては、
①製品開発しているネットワーク接続機器環境の健全性確保
②生産・品質検査しているネットワーク接続機器環境の健全性確保
③ERP、SCM、CRM との情報連携における健全性確保
④出荷した製品のサービスをしている機器（PC など）及びソフト環境の健全性確保
と三つ考える範囲が存在すると考えられる。
制御システムで使用する製品の位置付けで必要とされるセキュリティ試験の項目と合格レベルについて、業界事情を踏まえながら、ハザード事例情報やセキュリティ技術に関する情報を見ながら、セキュリティ品質基準を各ベンダで決めて実施していく必要があると考えられる。また、それに関する情報を公開して、出荷した製品に対する対策サービスを実施していくことも考えられる。

２）エンジニア会社／システムインテグレータの役割り
エンジニア会社やシステムインテグレータの役割りとしては、
①システム設計をしているネットワーク接続機器環境の健全性確保
②社外作業で使用している機器環境の健全性確保
が考えられる。
仕事をしている業界業種の現場の事情に合わせて、生産システムに関するユーザ指針を守って、ハザード事例情報やセキュリティ技術に関する情報を見ながら、セキュリティ基準に対応した制御システムの試験法案作成や試験実施を実施していくことが考えられる。

さらに、エンジニアリングする制御システムについて、ベンダとユーザの間で、どのセキュリティレベルが必要かの実施レベル調整を行って、取り決めていく実際の推進者となる役割が課せられることが増えてくるだろう。

3）エンド・ユーザの役割り

エンド・ユーザの役割り範囲としては、

①製品開発しているネットワーク接続機器環境の健全性確保
②生産・品質検査しているネットワーク接続機器環境の健全性確保
③ERP、SCM、CRM との情報連携における健全性確保
④採用している設備や装置の保証確保

が考えられ、①から③までは、ベンダ／メーカと項目は同じであるが、Supplier と User の立場の違いで責任の持ち方が違ってくる。それが④に現れてくる部分でもあろう。

制御システムと生産システムと一般業務の各ネットワークでのセキュリティレベルと管理基準の指針を決めて、関係者に公開し、その徹底に努力し、責任を持つことが求められる。

また、各ネットワーク間には、ゲートウェイを設置して、通過できるデータのみが取り合いできるようにするべく、予算を確保して、実施していくことが必要と考えられる。また、採用する主要な制御装置・ソフトアプリケーションにおいては、メーカ／ベンダやエンジニアリング会社との間で、Supplier Audit 契約が必要と考えることもあろう。

4）共通していること

一般業務では、様々な情報を入手することも必要で、インターネットアクセスをしない訳にいかない時代である。

製造業に関わる企業では特に、会社所有の PC およびネットワークの品質管理の指針を見直して、セキュリティに関する社員のモラルやスキル教育を実施し、それを守っているかどうかの監視も日頃必要であると考えられる。

セキュリティ品質管理に関わる者は、セキュリティに関する情報を入手するべく、その情報入手ソースを確保し、指針や基準の見直しに関するアクションを怠らないように心がけていく必要があるであろう。

6．低コストでできる制御システムセキュリティ対策

生産設備柔軟性と投資効果を考慮するとオープン化と標準規格採用を選択となるが、セキュリティ対策はこれとは異なる視点になる。

セキュリティ対策は、利便性とリスクのバランスを考えて、投資することになる。高度な利便性を求めるのであれば、セキュリティ対策は、専門のベンダに相談することが良いと思う。

不便であっても制御システムを守りながら、生産を継続していきたいのであれば、以下の対策を施して管理するのも良いと考えられる。

制御情報／制御系ＬＡＮでは、ＯＡと同じセキュリティは、困難である。では、どうするべきかであるが、

- リスクを認識する
    - ■ 「仕方がない」では済まされない！
      もし侵入されたら「どうなるのか？」事実を知る

次に

- ■ 攻撃されるポイントを認識する
    - ◆ 対策可能なら対策を実施
    - ◆ 対策不可能なら、監視をする

という話が重要となる。

となると無菌室状態を作るしかない。そこで、

- ■ 部外者を立ち入らせない
- ■ 持ち込みＰＣを接続させない
- ■ ＯＡ側からアクセスさせない
- ■ インターネットにアクセスさせない
- ■ 外部メディアの使用禁止

が、ポイントとして考えられる。

７．まとめ

整理すると、

１）社員教育の徹底

セキュリティ・ハザード事件を紹介して社員スキルを上げる。

業務の PC／USB を私用化しない躾が重要である。

２）生産システムで使用している PC は、インターネット接続させない。

３）インターネットにつながった Windows 系／Linux 系 PC と制御システムコントローラの直接／間接接続を避ける。

４）制御システムコントローラのコンフィギュレーション・ファイルのマスタ管理用の PC は専用にする。他への転用はしない。

５）生産システム（制御システム）と業務管理のネットワークは分けて、データの授受する段階での媒体（USB メモリなど）デバイスチェック用の PC を用意して、ビールスチェックを実施。これを徹底する。

６）外部関係者の PC は、持ち込まない。使わせない。

メンテナンス用の PC を用意し、作業はこれを使用する。この PC は持ち出さない。転用させない。

７）操作画面に権限区分をつける。

操作者 ID 情報と操作ログを自動記録する。

（記録していることで抑止力となる。）

が考えられる。

特に、システムのメンテナンスやテストの為に、三文字／四文字の簡略頭文字や test とか maintenance、supervisor などのありきたりのパスをそのままにしていると危険であることを認識する危機管理認識教育から始める必要がある。

以上

参考にした資料やサイト：

・２００９年度経済産業省情報セキュリティ政策局と JPCERT 主催「制御システムセキュリティワークショップ・カンファレンス」での発表資料

制御システムセキュリティワークショップ２００９（ http://www.jpcert.or.jp/ics/workshop2009.html ）

制御システムセキュリティカンファレンス２００９（ http://www.jpcert.or.jp/ics/conference2009.html ）

・VEC 主催“第２９回 VEC 協賛セミナー”での XML コンソーシアムセキュリティ部会発表資料

・XML コンソーシアム　Web サイト（ http://www.xmlconsortium.org/ ）

・　IA 懇談会主催“MOＦ２００８”合同デモシステム向けセキュリティ報告書

（ http://www.xmlconsortium.org/public_doc/mof2008_security/mof2008.html ）

・JPCERT　Web サイト（ http://www.jpcert.or.jp/ ）

・ＩＰＡ　独立行政法人情報処理推進機構セキュリティセンター

（ http://www.ipa.go.jp/security/fy20/reports/ics-sec/index.html ）

重要インフラの制御システムセキュリティとＩＴサービス継続に関する調査報告書

（ http://www.ipa.go.jp/security/fy20/reports/ics-sec/rep_main_fy20.pdf ）