［2012年度全国大会特別講演］

身近になった制御システムのセキュリティ
～見えない危機への備え～

小林 偉昭

この記事は，第8回情報システム学会全国大会・研究発表大会（2012.12.1）における特別講演の口述内容をまとめたものです。

今日は、制御システムのセキュリティが身近になったことを皆さんにどう感じていただけるか楽しみです。サブタイトルに「見えない危機への備え」と付けています。私はセキュリティをやっているので、サイバー攻撃がどのように変わってきているか、皆さんに少し感じていただければと思っています。

私は IPA で働いているのですが、今年 3 月にできた技術研究組合制御システムセキュリティセンターでも制御システムの活動をしていますので、その辺を踏まえて幾つかお話しさせていただきたいと思っています。

1. IPA の紹介

IPA は経済産業省所管の独立行政法人で、四つのことを行っています。私はその中のウイルス・不正アクセスや脆弱性の対策をセキュリティセンターで担当しています。IPA は研究機関ではなく、4 年ほど前から組込み機器（制御システム）などの新しいシステムに対するセキュリティの課題を調査して、成果を普及啓発している組織です。

Hideaki Kobayashi
独立行政法人情報処理推進機構（IPA）
技術本部セキュリティセンター
情報セキュリティ技術ラボラトリー
ラボラトリー長
第8回情報システム学会全国大会・研究発表大会［特別講演］
2012 年 12 月 1 日受付

2. 社会インフラへのセキュリティインシデント事例

社会インフラを重要インフラと言う人もいますが、これは皆さんの日常生活あるいは日本のいろいろな産業基盤を支えるものです。

2007 年に「ダイ・ハード 4.0」というサイバー攻撃をネタにした映画がありました。見た方もたくさんいるのではないかと思います。私も仕事柄見たのですが、先ほどの講演にもあった放送、テレビ各局の情報をジャックするという場面も映画の中にありました。米国政府のセキュリティ関係の仕事をしていた人が携わったサイバーテロであり、狙いは最終的にはお金だったわけですが、こういうことが映画にもなるほどでした。

これはいたずら的な事例ですが、道路の脇にある信号機に「CAUTION! ZOMBIES! AHEAD!!!」と表示されました。表示内容を変えるためのパスワードがあるらしいのですが、デフォルトで誰でも使えるようになっていました。

2 番目のいたずらは少しひどくて、ポーランドの電車好きの子どもが線路のトラックポイントを動かして、実際に事故が起きてけが人が出てしまいました。

3 番目は、ここまで来ると社会的にだんだん影響を及ぼしますが、原子力発電所の制御システムにワームが侵入し、原子力システムのいろいろなところが長時間にわたり動かなくなってしまいました。これはウイルスを広げるという悪意はあるのですが、この原子力発電所を狙ったわけではありません。

セキュリティを考えるときに「脆弱性」という言葉があります。ソフトウエアは機能を実現するわけで、その機能ができていないことを「バグ」と言いますが、攻撃者が一方的に攻撃する弱点を脆弱性と呼んでいます。その脆弱性を狙ってウイルスが悪さをするのです。

最後の例ですが、2010 年にイランのナタンツにある原子力施設の遠心分離機が壊れてしまいました。遠心分離機をコントロールする PLC（Programmable Logic Controller）という制御システムの上位に、Windows 系のいろいろなサーバーがあるのですが、そこの脆弱性を狙って入り込まれ、2 段階に分けて分離機の回転速度の数値をゆっくりと動かすコマンドを入力されてしまいました。普通は監視する人が異常を検知するのですが、その異常検知を逃れるため、機械が異常な値を教えてくれても正常な値に置き換えて監視盤に表示させていたので、監視している人も現場で機械がどう動いているか分からなくなってしまったのです。これはスパイ映画のように、現場の正常な写真を撮ってビデオで流し、その間で悪さをするのと同じような考え方です。「標的型攻撃」という言葉を最近使っていますが、特定の施設の特定のシステムを狙います。このウイルスはグローバルにばらまかれていますが、構成をチェックして関係ないと動きません。こうした標的型攻撃という非常に怖いものが 2010 年に出てきました。これは制御システムに対する 9.11 サイバーテロとも言われています。

身近な自動車や医療機器、情報家電などについても事例があります。ワシントン大学の Kohno 先生が、2010 年ごろから実験システムで自動車をいろいろさわっていたところ、自動車の中にある CAN（Controller Area Network）という LAN の ECU というコンピューターデータにいたずらができました。2011 年にはリモートでもできるようになりました。このようなことが起こると自動車が急に停止したりして、人命にも影響します。

2011 年に Black Hat という、セキュリティ専門の人がラスベガスに集まって議論する場がありました。医療機器のインスリンポンプ制御システムに侵入して量をおかしくすることができるという発表がありましたが、これも人命に関わる影響です。

少し古いのですが、HDD レコーダーが踏み台に使われる例もありました。

それから、次はビルをハッキングするという例です。

インベーダーゲームです。要するにビルを制御する機械にいたずらすることにより、こういうこともできるというのが現実のところです。

3. 制御システムおよびサイバー攻撃の現状と対策

制御システムはセキュリティ上、これから非常に問題になるということで、IPA は 4 年ほど前から欧米やアジアなど、状況を調査して、報告書として皆さんに提供しています。制御システムは、センサやアクチュエータ等のフィールド機器、コントローラ、監視・制御用に用いるサーバーやクライアント PC などをネットワークで接続した機器群（システム）と定義しています。

以前は情報システムと制御システム、本社と工場はつながっていませんでしたが、最近はネットワークでつながっています。ネットワークでつながっていなくても、USB を介していろいろなデータが工場に持っていかれています。従来、制御用機器は独自仕様のものが使われていたのですが、最近は汎用 OS など、汎用的な TCP/IP やイーサネットが使われるようになってきました。

「オープン化」という言葉がありますが、汎用製品と標準プロトコルが使われる環境に変わってきています。あまりソフトウエアが絡まないところもありますが、PLC のあたりが独自のものと標準のものとの境になっています。

その上の方はWindowsやLinuxになっています。

経産省の調査では、外部ネットワークとの接続は 36.8%で、ビジネス上のスピードや効率などでつながざるを得ないというケースになってきています。OS 環境は Windows や UNIX を使っているという状況となっています。

セキュリティから見ると、共通プラットフォームの利用により、Windows の脆弱性から、先ほどから言っているような攻撃がしやすくなっています。それから、利便性からネットワークへ接続しているので、ネットワークを介して遠隔からいろいろな攻撃ができます。さらに最近は無線の利用も増えているので、そこも狙われやすい。制御システムは 10～20 年と長い間使うし、かつ社会のインフラなのでなかなか止められません。そうするとセキュリティ上の問題で脆弱性があり、ソフトウエアを修正しなければいけないのですが、止めて直す機会がなかなかありません。いろいろな課題がある中で、これからどうしていくかを考えなければいけません。

「制御機器はインターネットに公開されていない」と普通の経営者は言うのですが、実はリモート管理の関係からつないでいたり、実際の構成は現場任せですので、本当は外につながっているのに分からないというのが現実のようです。

SHODAN（ショーダン）というツールを使うと、インターネット上で IP アドレスが見えるかどうかをチェックでき、それが制御系のものかどうかも分類できるそうです。米国の国土安全保障省（DHS）の方は「2 万以上の IP が外に見えるようになっている」と言っていますので、サイバー攻撃が現実のものになってきたら、経営者も自分のシステムがどういう環境になっているかをきちんと押さえる必要があると思います。

一般的な制御システムの構成図です（添付図参照）。下の制御システムに対しての攻撃としては、装置や設備の破壊があります。先ほどの Stuxnet のイランの例は、こういう設備の破壊を狙った攻撃です。それから、生産管理のデータを操作することにより、悪品質製品の生産や生産の暴走が起きてしまい、装置ベンダーの信頼失墜になってしまいます。日本の工場はほとんどコンピューター化されていますが、そこに USB でウイルスが入ってきて操業が 1 日止まってしまったことが現実にあるようです。自分のところで起きたとは外に対してなかなか言わないので分からないのですが、そういうところでもアンチウイルスベンダーの仕事があるという時代だと思います。

他の例では、画面は正常に表示し、異常コードをコントローラへ送るというものです。イランの原子力の話ですが、Stuxnet により、分離機に対する指令を出している PLC に変なデータを送ると異常が起こります。それをどこかで監視しているのですが、悪いウイルスが入って異常が起きているにもかかわらず、何も起きていないように見えるということで、非常に怖い話です。

もう一つ、現場でもハードウエアが劣化してしまったり、バグで止まったりすることがあるのですが、それらとサイバーの攻撃による異常とをどう切り分けるかが、今、制御系の非常に大きな課題となっています。先ほどから何度も脆弱性と言っていますが、海外の研究者が、従来の情報系のサーバーやパソコンだけではなく、制御システムの脆弱性を探してベンダーに修正を依頼するという動きが増えています。脆弱性がどんどん増加しているということで、2010 年ごろから脆弱性に対する関心が増えています。

Stuxnet を考えると、非常に高度な攻撃のソフトウエアが作られています。一般のいたずらではなく、裏には国があるのではないかとか、大きな組織があるのではないかなどと言われています。実はそういう攻撃は 2003 年ぐらいから既に起きていて、それが 10 年以上にわたり、APT（Advanced Persistent Threat）といってしつこく続いています。例えば米国ではボーイングやロッキードなど、軍需産業のシステムに何らかの形で入り込んで情報を窃取しようとしています。窃取の行動はずっと続いている

のですが、Stuxnet は窃取だけではなく破壊攻撃もするようになってました。このようなサイバー攻撃による被害はこの 2 年で非常に増えてきています。

これについても有識者と研究会をつくり、「新しいタイプの攻撃」の流れという形でまとめました。スパイ映画とほとんど同じで、ターゲットの情報を取るために、ターゲットの企業、働いている人、どういう人と付き合っているかなど事前の調査をします。

初期潜入段階としては、ファイアウォールなどがあるとなかなか入りにくいのですが、電子メールに変なものを付けて送ったり、USB メモリ、あるいはウェブサイトにアクセスしてもらい、そこに変なものを入れておくというように、いろいろな形で潜入しようとします。2 番目は攻撃基盤構築段階ですが、いったん入り込むと、そこから C&C サーバーと影で通信しながら攻撃の基盤をどんどん確立していきます。その後、システム調査段階では、このシステムの中にはどのようなお宝情報があるか、いろいろなことを調べます。そして、調べ終わると、最終的にそのお宝データを盗みます。こうした流れは、Stuxnet 以降、Duqu や Flame なども大体同じ形です。

「もし起きたら」を考えた対策が必要です。USB を差すことによりウイルスに感染してしまいますが、その後、例えば工場の現場に行って USB を利用すると、その中のウイルスが悪さをすると、生産ラインが停止してしまい、サプライチェーンなど次の会社に迷惑を掛けてしまうことになります。ですから、これは人ごとではなく、きちんと考えていかなければいけません。

対策としては、不正侵入検知、アンチウイルス、ファイアウォールなどで守っています。悪いウイルスが入るとファイルを壊してしまったりするので、入り口で防ぐのですが、それをすり抜けてしまうものもあります。潜入したウイルスが外部のサーバと通信して、さらに強力に成長して、その結果、情報を持っていくわけですが、出口でのやり取りをうまく抑えてしまえば実害は起きません。一つの発想として、入り口で守り、出口でもきちんと守ってほしいというのが IPA からの発信です。

そういうことを整理したものが「八つの出口対策」です。ネットワークの構成を切り替えてもらうなど、いろいろな話をまとめた「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」もあるので、これを見て少し考えていただければと思います。これについても今後新しい対策を追加していこうと思っています。

4. 制御システムのセキュリティ向上への取り組み

米国のアイダホにある INL（Idaho National Laboratory）という研究所は、DHS（国土安全保障省）と一緒に制御システムに対するサイバー攻撃の対策技術にきちんと取り組んでいこうという活動をしています。ベンダーのシステムを実際に攻撃して、その対策技術をきちんと研究していくという形を取っています。米国でも制御システムの事業者は、これからサイバー攻撃対策は重要だといくら言っても、サイバー攻撃など来るはずはないといって動いてくれませんでした。認知してくれないので、2007 年にオーロラ・プロジェクトということで、発電機にサイバー攻撃のコマンドを入れることにより異常動作を起こし、実際に発煙して壊れてしまうところをビデオに撮り、このような危険があると PR しました。インターネットで「オーロラ・プロジェクト」と検索すると映像が出てくると思います。

何が言いたいかというと、サイバーはコンピューターのソフトウエアをおかしくするだけではなく、Stuxnet と同様にハードウエアの異常動作にも結び付くということです。2007 年に作ったビデオを、米国の国防関係でイランの原子力開発を気にしている人たちが見て、このようなアイデアもあるのか、イランのシステムをサイバーで攻撃したら原子力の分離機に異常を起こせるのではないか、米国政府がイランの核開発を遅らせるために作ったのではないかなどという記事が、2012 年 6 月 1 日に「ニューヨーク・タイムズ」に出ました。記事ですので正確かどうか分かりません。いたずら

から、軍事あるいは経済に影響するものもあります。情報窃取はどちらかというと経済面が多く、特に中国からの攻撃ではと言われています。

Stuxnet の件を受けて、日本では経済産業省が「サイバーセキュリティと経済研究会」を立ち上げました。主な検討項目は標的型サイバー攻撃や制御システムの安全性確保がこれからは必要だということを提言しました。それを受けて、翌年「制御システムセキュリティ検討タスクフォース」を立ち上げました。ここでの目標は、日本国内の ICS（産業用制御システム）セキュリティ確保です。日本の社会インフラを支えている制御システムをセキュリティ面からも強いものにしていくことは、日本の産業力向上や国民の安全のために必要です。もう一つは、ベンダーが海外に製品を輸出するときに、国際規格に対応したセキュリティを標準的に実装していくことです。現実に、海外の石油メジャーなどは、制御システムや製品を調達するときにセキュリティの基準を設け、それに従ったものを納品するという動きになってきています。

こうした活動を受けて、今年 3 月に技術研究組合制御システムセキュリティセンター（CSSC）ができました。「セキュアな制御システムを世界へ未来へ」という目標を作っております。新誠一先生が理事長で、事業者としては森ビルが参加してくれています。あとは電力、ガスなどこれからいろいろ広げていくと思いますが、現状は 13 組織が加盟しています。お台場の産総研の中に本部を置いていますが、テストベッドを宮城県多賀城市に構築しているところで、スケジュール的には 2013 年 3 月に完成予定です。テストベッドを中心に、技術の確立、普及啓発などいろいろなことをしていこうと考えています。

組織には、研究開発・テストベッド委員会など四つの委員会があります。評価認証・標準化委員会は、新先生が委員長で私が副委員長です。インシデント・ハンドリング委員会は、制御システムの脆弱性を情報システムと同じように公開していいのか、24 時間 365 日動かしているので、公開したからといってパッチ対策をすぐにできるわけではなく、システムは直せません。制御システムのベンダーは利用しているユーザーは全部抑えていて、自分たちで全部チェックしているから公表する必要はないと言っています。新しく脆弱性を発見した場合にどうするか、インシデントが起きたときにどのような支援体制を作ればいいかということも検討しています。

CSSC は宮城県多賀城にあるソニーのワンフロアを借りています。テストベッドにはまだ何も入っていませんが、PA、FA、BA を対象とした模擬プラントを構築し、それを使ってセキュリティの検証をしたり、演習したりすることを考えています。特に管理者層にも見てもらいたいです。サイバー攻撃を受けて、プラントがおかしくなるとどのような現象が起こるか、臨場感を持って分かるような形で教育していきたいと考えています。

経営者も含めて制御システムを分かっている人にセキュリティもさらに分かってもらいたいということで、普及啓発や人材育成をいろいろ考えてはいるのですが、日本のレベルはそこまでいっていません。INL ではブルーチーム（守り）とレッドチーム（攻撃）いう二つのチームに分かれてお互いの技術を磨いているので、日本でもそういう形のものを構築して、日本の人材育成を図っていきたいと思っています。

それから、製品を海外に出すときに、やはり標準に準拠していることを印として付けると流通しやすいので、評価認証スキームの実現も現在進めています。

世の中には、制御系のセキュリティに対してシステム、コンポーネント、技術、それから業界などいろいろな標準があります。北米の電力システム用には、CIP という形でいろいろな規格を作っています。われわれが着目したのは IEC62443 です。業種にはあまり関わらない、かつ組織、システム、コンポーネント全般にわたる標準をこれから普及していく必要があるのではないかと考えています。位置付けとしても、管理面などいろいろ幅広いところをやっていきます。

IEC62443 は四つのレイヤからできています。1 番目が総論です。2 番目が管理・運用・プロセスで、ターゲットは事業者、アセットオーナー、電力会社やガス会社などです。ISMS（Information Security Management System）は、オフィス系のセキュリティについてマネジメントするものですが、工場関係のマネジメントをきちんとするのが 2 番目のシリーズ CSMS（Cyber Security Management System）です。3 番目は、まとまりのある制御システムについてのセキュリティを守るもの、4 番目はコンポーネントで、製品ごとのセキュリティ標準を決めたものです。

IEC62443 には 12 個の標準があります。既に国際標準、IEC の標準になっているものを普及するために、IPA は 10 月 10 日に規格協会から翻訳したものを出版しています。2-1 のマネジメント関係については、ガイドラインという形で分かりやすくしたものも一緒に出しているので、インターネット上で見ていただきたいと思います。

このように、制御系のセキュリティについてもかなり国際標準が進んでいます。多分 2014 年ぐらいには標準がある程度固まると思っています。

ベースとなる標準と認証をするための規格があります。認証の規格を定めているのが ISCI（ISA Security Compliance Institute）で、認証のプログラムを作っています。EDSA（Embedded Device Security Assurance）は 3 種類の規格で作られており、将来的には IEC の 4 番目のシリーズになると思います。

認証について、ISCI は 3 種類の評価をしています。CRT（Communication Robustness Testing）は、通信レベルでの評価です。基本的にはファジングというランダムなデータをぶつけて、矛盾が起きないかを見ます。FSA（Functional Security Assessment）は、セキュリティの機能についての評価、SDSA (Software Development Security Assessment) はソフト開発プロセスの評価です。この三つを、レベル 1、レベル 2、レベル 3 という形で規定し、現在は米国の 2 社の四つの製品がこの認証を取っています。

そのフレームワークですが、ISCI という全体を推進する機関が、評価・認証機関を立ち上げて、そこにベンダーが製品評価を申請して、テストしてもらいます。ここを評価・認証機関としてきちんと認定するために、米国には ANSI と ACLASS があります。使うテストツールについても、ISCI がきちんと承認するというようなフレームワークになっています。

当然、海外に行ってこれを取るのではなくて、日本でも取りたいという要求があります。日本の評価認証機関で取ると国際的に相互に認証し合うという形を狙って、今、CSSC（Control System Security Center）を中心にフレームワークの構築について一緒に検討しているところです。CSSC の中の委員会で、実機を使って試験検証し、ノウハウを蓄積しながら、ISCI の認証プログラムの内容を現在習得しているところです。

目標としては、2014 年 4 月から実際に日本でもサービスができるようにということで、現時点ではいろいろ勉強しています。2013 年に 1 年間試行して、実際のサービスは 2014 年 4 月から開始し、国際的にも相互認証ができるような形で進めているところです。

コンポーネント（制御機器）の話をしたのですが、もう一つ、SSA（System Security Assurance）があります。実際の事業者やベンダーは、コンポーネントを売りたいのではなくて、やはりシステムを売りたいのです。従って、システムのセキュリティをきちんと認証できるような仕掛けということで、SSA というシステムセキュリティのアシュアランスがあります。IEC62443-3-3 のシリーズに最終的にはなると思いますが、これが今 ISCI でも検討されていて、多分年末ぐらいにはできるようになるのではないかと見ています。いつも遅れ気味なので、年明け春頃にはシステムの認証サービスが米国で実施されるのではないかと思います。

もう一つ、マネジメント関係ですが、ISCI はここをやるつもりはないようです。日本では日本情報経済社会推進協会（JIPDEC）が認定

機関になっていて、JIPDEC の ISMS の活動の中で、一般のオフィスだけではなく工場もこの規格に従えばいいのではないかということで、今、検討をしてもらっているところです。ただ、情報システムと制御システムは、やはりリスクの考え方が違うと思います。IEC62443 でも HSE（Health・Safety・Environment）ということで、人の健康も考えなければいけません。それから安全性をどう考えるか、環境に対する影響をどうするか。そのリスク分析もして、それに対してどうマネジメントするかという、その追加の部分が多分出てくるだろうということで、その辺を明確にして皆さんには使ってもらいたいと思います。

5. IPA の活動

IPA が考えているのは、企画から設計、実装、テスト、運用/利用、最後には廃棄というシステムのライフサイクルです。データが入ったものをそのまま捨てるのではなくて、安全に捨てる。そういうフェーズに対して、どのようなセキュリティ対策が必要かを考えて活動しており、それについて成果物も出しています。

例えば、「組込みシステムのセキュリティへの取組ガイド」では、16 の具体的なチェック項目で、企業が今どのレベルにいるかを確認できます。担当者はセキュリティを全然考えていない、担当者はある程度セキュリティを考えている、部門としてきちんとセキュリティを考えている、あるいは企業として全体のセキュリティを考えているというように、どのようなレベルにいるかチェックしてもらい、一つ上のレベルに上がるためにはどのようなことをすればいいかをまとめています。制御システムについても参考になると思います。

最近の活動としては、サイバー情報共有イニシアチブ（J-CSIP）があります。去年の秋ごろ、重工・防衛産業をはじめ、原子力など国のインフラを支える企業で、標的型メール攻撃による情報漏えいがありました。これは 1 社だけ狙っているのではなく、同じ業種を狙っています。重工業 9 社でスタートしましたが、9 社の誰かのところに標的型攻撃が来たら、その情報を IPA に届けてもらい、IPA はその情報を匿名化して残りの社に提供します。IPA は秘密保持契約（NDA）をそれぞれの企業と結び、きちんとした情報管理をしながら活動しています。

それから、「脅威と対策研究会」は先ほどのガイドブックを作った研究会ですが、ここはオープンな環境で人が集まり、いろいろディスカッションしながら、その成果を公開していくという形で活動しています。昨日もこの研究会を開催し、160 人であるテーマについてディスカッションしました。

IPA は安心安全相談窓口を持っているので、標的型メールが来たらそこに届けていただくと、それを解析して皆さんに注意喚起します。今、銀行で問題になっているのは、ポップアップでメニューが開き、コードなどを入力すると全部盗まれてしまうというものですが、その検体を分析して注意喚起しています。

脆弱性は日々見つかっていますが、最低限皆さんにもできることは、脆弱性の対策をした最新のソフトウエアを常に使うことです。マイクロソフトは自分のシステムについてはネットワーク経由で直しに来て、自動的に更新してくれます。ただ、それ以外の PDF などはなかなか気が付きません。全てではありませんが、皆さんが使っているものについて簡単にチェックするツールがあります。最新のソフトか、そうでないかをチェックし、最新でなければそれをダウンロードして新しいものにするように表示する「MyJVN バージョンチェッカー」というものもあるので、お使いいただきたいと思います。

セキュリティ情報は経済産業省や総務省、内閣官房、各ベンダーなどいろいろなところから出ているのですが、それら全体のポータルをきちんと確立していこうとしているのが「ここからセキュリティ！」というサイトです。

IPA が昨年 8 月から行っている一つのセキュリティテスト手法として、ファジングという手法があります。既に分かっている脆弱性は当然対策しなければいけませんが、悪い人は未知の脆弱性を使って攻撃してきます。未知の脆

弱性を見つけるのによく使われるのがファジングというツールです。悪い人が使っているのに、なぜ守る人がそれを使わないのかということで、そこを皆さんにきちんと使ってほしいのです。ただ、テストには期間がかかります。製造現場の方からは、忙しい期間にこういう作業を入れ込むのは非常に大変だと言われます。それは分かるのですが、早めに見つけて対策すると、それだけ後で費用なども効率化できるのです。IPA はこうしたツール利用のしおりなども作っているので、これも見ていただくといいと思います。

先ほど杉野会長の話の中で、人間をどのように使っていくかということでしたが、われわれ脅威と対策研究会も、システム全体をどう分析して、そこでどう守るか、悪い人は今どのようなことを考えて、何をターゲットにしているかといったことについて、人間が集まってインテリジェンスを共有していかないと攻撃者に対抗できません。単に製品を置けばいいということではなく、設計の段階から皆さんと情報共有をしていく必要があるのではないかと思っています（拍手）。

添付図