PSB
(Process Safety Beacon)
2021 年 7 月号
の内容に対応

SCE・Net の
安全談話室(No.181)
http://sce-net.jp/main/group/anzen/

化学工学会
SCE・Net
安全研究会作成
(編集担当:竹内　亮)

サイバーセキュリティと化学プラントの運転

(PSB 翻訳担当:春山　豊)

司会　：　今月号は、サイバーセキュリティがテーマとなっています。今年5月に米国のパイプラインがランサムウェアの攻撃を受けてガソリンの供給が滞ったことも今回の Beacon に記載されていましたが、サイバーセキュリティはプロセス安全にも身近な問題になって来ています。まず、今月号の Beacon についてご感想をお聞きかせください。

木村　：　米国のパイプラインの事例もかなりの話題となりましたが、今回のフロリダの事例では生活インフラ「水道水」が狙われたことからも、サイバーセキュリティの脅威がより身近な問題としても迫ってきていることを実感いたしました。また，数年前に NHKTV で放映されたネットに繋がった医療機器のヤバすぎる実態「点滴装置の乗っ取り」の映像が思い出されました。

竹内　：　木村さんから送って頂いた NHK スペシャルの記事には、医療用のレンタル機器を返却する時にその機器に設定したパスワードを消去しないことでパスワードが流出して、他の装置のパスワードも共通にしていると乗っ取られる危険があることが記されていましたね。サイバー攻撃がそんなところまで来ているのかと驚きました。

金原　：　最近は手口が巧妙になってきており、イタチごっこの様相を呈しています。今回はオペレーターが早期に発見し、冷静に的確に操作したことにより大事に至らなかったようです。後から考えればそういうことだったのか、と思うでしょうが、渦中に巻き込まれているときは何が起きているか分からないだけにオペレーターの能力を高めることや日頃の訓練が大切であると考えます。今回は1点での異常だからまだよかったのかもしれませんが、多点攻撃されることを考えるとぞっとします。

竹内　：　Beacon の水道水の事例は、たまたまオペレーターが画面を見ていた時に NaOH の濃度の書き換えが行われたので、直ぐに気付いて対応出来ましたが、見ていなかったら実害が生じていたと思います。たまたま見ていたというのはラッキーだったと思います。しかし、その後、どうしたかも気になりますね。

山岡　：　「知っていますか」の最後に「サイバーセキュリティの穴の95パーセントはヒューマンエラーが原因」とありますが、ヒューマンエラーが95パーセントというのはちょっと理解できません。この95パーセントには何が入っているのでしょう。例えば、サイバーアタックがセキュリティに先行しているために被害を受けるというケースはどちらに入るのでしょうか。

木村　：　私も95パーセントが何を指しているかは分かりませんが、USB の持ち込みなど、色々なきっかけはあると思いますが、意図していなくてもサイバー攻撃に関与してしまうようなことも含めていると思います。

竹内　：　フィッシングに引っかかるとか、USB メモリーのセキュリティチェックをしないで使ってしまうなども、人のミスだと思います。おそらく、被害を受けた時に検証してみたら、何か人のミスが絡んでいたという割合が、95パーセントあったということではないかと思います。ただ、システム自体も人間が作ったものですので、そう捉えると全て人のミスに繋がりますね。

山本　：　そうですね、Beacon の参考資料を見ると、サイバー攻撃の最も一般的な原因は、インターネットに放たれたマルウェアを人間がダウンロードしたこととあります。最近は工場の効率化で化学プラント内の情報をIoT（Internet of Things）技術で集めて分析することが多くなっていますので、サイバー攻撃の防護対策は、インターネットを使用する社内の従業員全員が対象になりますね。

牛山　：　「システムは人間の作ったものだから必ず弱点がある」と言うのが、ハッカーたちの考えだそうですね。やはり、現場の人も含めて一人一人が気を付けて対応しなければならないのだと思います。

司会　：　これまでに、プラントに対するサイバー攻撃について経験されたことや見聞きしたことを教えて頂けますか。

今出　：　直接経験したことはないのですが、海外の事例では 2010 年イランの核燃料施設への攻撃でウラン濃縮用遠心

分離機の稼働不良、2012 年米国の電力会社がマルウェアの感染によって運転再開が 3 週間遅延したこと。2017 年中東の石油プラントの安全計装システム（SIS）への攻撃で緊急停止した、などがあります。 その他水道、鉄道、病院などに対しても事例があり、社会基盤へのサイバー攻撃の脅威が高くなっていると思われます。

金原 ： 私も直接経験したことはありません。今出さんが話されたイランの核燃料施設の SIS の攻撃では、マルウェアが SIS コントローラーと通信でき、プログラムを改ざんすることができる機能を持っていたそうです。攻撃の過程で攻撃側がミスをして誤ってシャットダウンさせたとのことです。本当に恐ろしいことまでできると驚きます。

木村 ： そのサイバー攻撃では遠心分離機の回転数を上げて壊そうとしていたが、作動不良で止まってしまったと書いてあったと思います。

今出 ： 日本では、顧客データの漏洩など情報システムの事例は話題になることがありますが、制御システムへの攻撃についての情報はあまり報道されていないようです。情報が少ないので内容はよくわからないのですが、自動車の生産ラインの処理能力低下、半導体工場の生産ラインの停止などがあったようです。既にサイバー攻撃はある程度の頻度で起こっているのかもしれません。

竹内 ： 自分の所がやられましたとは、言い出さないのかもしれませんね。

木村 ： IPA 独立行政法人情報処理推進機構セキュリティーセンターの資料「制御システムのセキュリティリスク分析ガイド第2版（2020 年 3 月版）～セキュリティ対策におけるリスクアセスメントの実施と活用～, 2020 年 3 月」https://www.ipa.go.jp/security/controlsystem/riskanalysis.html を見ると付録 C. 制御システムのインシデント事例にサイバー攻撃の実例が沢山リストアップされています。

今出 ： どのような経路で侵入されたかを共有できれば、防止に役立ちそうですね。

木村 ： 日本の化学会社では個々にはサイバーセキュリティ対応を図りつつあることが聞こえてきますが、具体的な対応の詳細はあまり見えてきません。そのような状況において、例えばI社では、社内の大規模ウイルス感染を契機に、制御系ファイアウォール設置、制御系ネットワークのセキュリティ対策要領制定から始まり重要インフラの情報セキュリティ対策に係る第3次行動計画（2014年）の策定に歩を進めています。そして現在では、サイバーテロ・サイバーインシデント訓練、セグメント・侵入検知、ホワイトリスト導入、ID 管理、インフラ・健全性監視を実施しているようです。また、A 社のように、サイバー攻撃への対抗策としてわが国では先駆的に論理的ネットワーク分離のために一方向性セキュリティゲートウェイを設置している事業所もあります。結論的には、IT 技術者とプロセス技術者の協力関係の重要性と両者の間の壁をなくすことに対する努力の必要性を強調することが求められますし、ネットワークを分離し同時に攻撃に陥落しにくいようにするなど、プロセス技術者の立場からサイバー攻撃からの防御を主体的に検討することが必要であるように思われます。

竹内 ： 一方向のゲートウェイは私もあるジョイントベンチャーで DCS の導入プロジェクトを担当した時に使用していました。情報を出すことは出来るが、外からは入れない仕組みですね。ところで、安全部会の新PSMの検討で3年くらい潜んでいて、それから悪さをするマルウェアのことを書かれていたと思いますが。

木村 ： あれは橋本先生が書かれた部分で詳しくは知りませんが、USB などを介して侵入して暫く潜んでいて時間が経つと悪さを始めるものがあるということを橋本先生が強調された文です。それから National Institute of Standards and Technology(NIST), IPA 独立行政法人情報処理推進機構翻訳監修 Framework for Improving Critical Infrastructure Cybersecurity, 重要インフラのサイバーセキュリティを改善するためのフレームワーク, Version l.1, April l6,2018. https://www.ipa.go.jp/security/controlsystem/riskanalysis.html も提案されており、具体的な産業用制御システム（ICS）セキュリティに関しては、NIST, JPCERT コーディネーションセンター翻訳, Guide to Industrial Control Systems (ICS) Security, Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC) 産業用制御システム（ICS）セキュリティガイド SCADA, DCS, PLC その他の制御システム設定, NIST Special Publication 800-82, Revision 2, May 2015.が活用できそうです。

司会 ： 皆さんの会社ではサイバー攻撃に対する備えはどうされていましたか。差し支えの無い範囲でお話しいただけますか。

今出 ： 務めていたのは米国の企業でしたので、日本に比べ早い時期から PC の管理やセキュリティ教育が実施されていました。 例えば PC、DCS やルーターなどのネットワーク機器は、社内で検査し・認定したメーカー、型番、ソフトウェアのみしか利用できないよう管理していました。 なお、情報システムは IT 部門、制御システムはエンジ

ニアリング部門が管理していました。IT 部門とエンジニアリング部門が協調して仕事をするのは大切だと思います。ハッカーたちも日進月歩なのでこちらも継続的な対応が必要です。

塩谷 ： 制御系システムは工場の計装エンジニアが担当して、遠隔監視やリモートメンテナンスなど様々な技術導入が図られ、制御系ネットワークも外部ネットワークと接続せざるを得ない状況になっています。制御システムのセキュリティ対策については、計装エンジニアに任せるだけでなく、IT 部門による助言や審査などの支援が必要となっていると思います。

竹内 ： 計装部門と IT 部門の協調は旨く行っていましたか?

塩谷 ： はい、ネットワークに繋がる様な時は、IT 部門に参加して貰って検討をしていました。リモートメンテナンスを導入する際は、DCS ベンダー側のセキュリティ対策を聴取・評価してもらいました。それから、制御システムのデータバックアップを定期的に実施することは重要です。定期的なバックアップを実施することで、サイバー攻撃をはじめとして種々のトラブルや事故からの早期復旧に役立ちます。

竹内 ： データのバックアップはサイバーセキュリティの面だけでなく、システム障害への対策として我々もしっかりとやっていました。ところで、DCS が導入され始めたころは DCS が信用されておらず、パネル制御も出来るようになっていたと思います。しかし、今は DCS の信頼度が上がってパネル制御を併用するケースは減っていると思います。

金原 ： あくまでもウイルス侵入防止への対応ですが、特に最近は「なりすましメール」と言って社内にいる人の名前を使ってメールを送り、添付ファイルを開かせてウイルス汚染させる手口があります。社内のイントラネットであれば、送信者欄に漢字で名前と部署が表示されるのですが、外部からインターネットで送信した場合は、アルファベットのメールアドレスしか表示されないので、注意が必要です。

竹内 ： はい、フィッシングメールは多くなっていますね。個人でもクロネコヤマトやアマゾンなどを語ったメールなどを受けることが時々あります。先日、私の知り合いから、佐川急便を名乗るフィッシングメールに騙されそうになったと聞きました。

金原 ： 侵入防止も大切で、それは各社各様に体制を組んで専門家を設けて逐次防止策を取られていると考えます。一方で、いかに防止策をとっても巧妙な手口で侵入してくる可能性は否定できません。侵入された時の想定されるトラブルをリストアップし、対応策を考え、そして日頃から訓練しておく必要があると考えます。かつて 2000 年問題(※)というのがありました。あの時はコンピューターが異常作動する可能性と想定される事象をリストアップし、いざというときに備え、訓練も行いました。結果的に大きな問題がなく過ぎましたが、システムの異常対応という意味で貴重な情報と知見を得たように考えています。(※)西暦 2000 年になると下 2 桁で年数表示している場合、コンピューターが 1900 年と誤って捉え、誤作動すると言われた問題。

春山 ： 金原さんの侵入防止のコメント大変重要な点です。10年ぐらい前に大手造船・機械の企業がサイバー攻撃を受け生産に大きな影響を与えた事例があります。その入り口が業界団体・行政関係部署の名前を使い重要事項としてメールを発信しその中にウイルスを埋め込んであり感染してしまった事例です。そのころ、協会関係の業務をしておりましたが業界団体の会員は大企業のみならず中小企業もあり、また各種団体もありますので、感染は瞬く間に広がる怖さを痛感いたしました。 サイバー攻撃に対しては個社のみならず協会団体、行政関係部署との連携強化が極めて重要です。また先ほど木村さんから紹介がありました IPA 等の専門家集団との連携も必要です。

司会 ： コンピューターの進化が著しく、DCS など計装システムもかなり複雑化していると感じていますが、PSM の観点からはサイバーセキュリティについてご意見はありますか。

今出 ： 以前の制御システムのネットワークは工場内で独立していたのですが、今は情報系のネットワークと繋がるようになり、汎用化した装置が増えたために、攻撃しやすくなっていると言われています。また、制御システムのセキュリティ意識や対策は情報システムに比べまだ低いのではないでしょうか。私が勤めていたころは、日本のメーカーの DCS はなかなか認められませんでした。セキュリティや PSM 対応、グローバル対応などがネックになっていたかもしれません。

塩谷 ： 過去に勤務していた工場では、DCS の故障に備えて、緊急停止システムはハードリレーで構築していました。近年のようにサイバーセキュリティの脅威が現実となっている状況では、重要度の非常に高い安全計装システムはDCS外のハードリレーによるシステム構築も考慮する必要があるかもしれません。

竹内 ： そうですね。私も PHA の結果、最悪の事態が極めて大きな事故に繋がる様なハザードについては、DCS による

安全対策だけではダメな時代になってしまったと思います。また、DCS の OS がメーカー独自のものから UNIX や Windowsに移行していることもサイバー攻撃を受けやすくなっていると思います。

牛山 ： UNIX や Windowsに移行する利点は何なんでしょうか?

竹内 ： それはオープンアーキテクチャーにすることで、多くの装置メーカーがその DCS に合わせた部品を提供できる点だと思います。

今出 ： そうですね。汎用性が上がることが利点です。しかし、Windows などは頻繁にパッチを当てていますが、なかなか脆弱性の問題は解決しませんね。

竹内 ： それに Windows の場合は、古いバージョンはマイクロソフトがサポートしてくれなくなってしまうのも問題ですね。

今出 ： そうですね。Windows XP が無くなった時は大変でしたね。

牛山 ： ところで、制御系と情報系とが繋がることが必要になったというのは、どういうニーズから生じているのでしょうか?

今出 ： 私の知っている限りは、生産システムや上位の管理システムと直接データのやり取りをするようになったためだと思います。

牛山 ： 確かに会社の中で、その様な情報を共有したいというニーズはあると思いますが、いわゆる経済情報に直結するデータは外部のシステムと切り離して構築することは出来ないのでしょうか?

竹内 ： 外部に情報を提供しなければいけないことはあります。例えば、ロットごとの製品の品質保証を行う場合、倉庫のシステムと連携して、どのロットがどの顧客に行ったかを確認して品質データを送るケースがありました。

牛山 ： なるほど、現場からデータを拾い上げてスピードアップを図るということはあるのでしょうね。しかし、それがサイバーセキュリティの脆弱性にもなっているのですね。

頼 ： 外部とのつながりの件ですが、加工型工場のシステムはかんばん方式に近く、こんな原料が来たらこちらの生産方法に変えようとか、顧客の要望に合わせて生産計画を立てて在庫を最小化しよう、などのことは20年も前から行われていましたので、今はもっと繋がりは密接になっていると思います。そう考えると、外部からの情報も生産にとって重要ですから、外部と完全に切り離すことは難しいと思います。

三平 ： 古いプラントの事例ですが、当時は他社からの製品を受け入れるのに他社の敷地内のバルブを遠隔で操作したことがあります。その時は、専用線で信号を送って操作していました。あの時の様にインターネットを使用しないで情報のやり取りが出来ればよいのかなと思います。

竹内 ： そうですね。専用線を使用していれば乗っ取られる心配はありませんね。しかし、インターネットを使用した方が安く実現できるので、そちらに飛びついてしまっているのだと思います。

金原 ： 異常の早期発見や、少人数化により遠隔地の情報を一元化管理するなど、運転管理はコンピューターなしではすまされない時代になっています。また防止対策が脆弱な監視カメラなどからも侵入するという情報もあります。それだけに、先ほど申し上げた、侵入された時の対策も必要です。DCS を分割して、例えば温度制御と液面制御のネットワークを分離し、片方が攻撃を受けてももう一つで制御できるなどの方策が提案されています。また、さらに手動操作で対応できるようにするなどの方策もあります。いずれにしてもオペレーターへの教育をいかに徹底しておくかがカギとなると考えます。

竹内 ： そうですね、誰もがサイバーセキュリティに関心を持たなければならなくなっていますね。ところで、最近はシステムが高度化して、自動車などのメンテナンスでも USB でデータを吸い上げて不具合のある個所を簡単に特定していますが、プラントの中でもその様なメンテナンスが行われているのではないでしょうか?

今出 ： 今、計測装置とかはインテリジェント化が進んでいて、遠隔から機器の状態をモニターしたり、データを取り出したり出来るようになっています。逆にそれには、外部からの侵入がしやすくなっている面がありますね。

竹内 ： USB などで、外部からソフトを持ち込む際に、持ち込んだ本人には悪意が無いのに USB メモリーにマルウェアが仕込まれているというケースもあると聞いたことがあります。USB のウイルスチェックをしても、セキュリティソフトに引っかからないことを確認したマルウェアが仕組まれていることもあるそうです。

今出 ： そうすると防ぎようがないですね。

竹内 ： 結論として、インターネットに接続された DCS はファイアウォールやセキュリティソフトなどで対策をしても完璧には外部からの侵入を防ぐことが出来ないのだとすれば、防護層としての DCS は 1 レイヤーであって、DCS 上で複数のロジックを組んでも防護層は増えないと考えておく必要がありそうですね。そうすると影響度の高いハザードについては DCS が機能しない、又は異常動作したとしても、安全弁などの DCS に依存しない防護層で守り

切ることを考えないといけないと思います。PHA では従来、ユーティリティの喪失は考慮して来ましたが、DCS の機能喪失も視野に入れる必要がありそうです。

司会 ： 昨今は、コロナウイルス対応でも働き方が変化しつつあり、DX(デジタル・トランスフォーメーション)などが取り沙汰されていますが、ご意見のある方はいますか。

今出 ： 一般的に日本はセキュリティに体する知識や意識がまだまだ低いと言われていますね。小学生のコンピューターの教育も始まっているようですが、プログラミングのテクニックだけでなく、セキュリティ や情報管理の重要性についても教育していくことが大事なのではないかと思われます。

木村 ： 情報系の教育は小学校でも本年度くらいからプログラミング教育が始まっています。スクラッチ(Scratch)やビスケット(Viscuit) というソフトウェアを用いて、ブロックを積んで何をやりたいかの自分の考え方をプログラムするといことを学びます。文科省の HP を見るとセキュリティに関する部分としては、情報モラルに関する事柄が 6 項目ほど挙がっています。また、大学の工学教育プログラムに関しては一般社団法人日本技術者教育認定機構(JABEE)が認定審査を担当していますが、情報分野のプログラムの名称に「情報・サイバーセキュリティ」というキーワードが数年前に入ってきました。

竹内 ： デジタル・トランスフォーメーションと言うと大げさかもしれませんが、安全研究会もこの様にオンラインで会議をして翻訳のチェックをしたり、議論をしたりがあまり問題なく出来ることが判りました。今後、コロナ禍が解消した後も、このままオンラインを続けることも可能かと思います。特に遠隔地のメンバーは学会の会議室に毎回参加するのは困難ですので、オンラインの方が便利ですし、会議の記録も録画できるので便利です。顔を合わせてのミーティングも魅力はありますが、この様なやり方に変わっていくのかなという気がします。

今出 ： そうですね。コロナで大分加速された感がありますが、アフターコロナにも影響しそうですね。

金原 ： 行政のデジタル化の加速のカギはマイナンバーカードの普及と言われています。マイナンバーカードはようやく申請が伸びてきたといっても、５月で 30%とのことです。私はカードを開始当初に発行してもらいましたが、今のところマイナポイントをもらう時に使ったくらいです。今後は様々なところで活用されるとのことなので期待しています。ただ、パスワードを忘れたといって窓口が混乱しているという話も聞きます。確かに私もあれこれとパスワードを持っており、それを定期的に変更してください、と要請を受けます。パスワードはノートに記入していますが、最新版管理が大変です。これからの時代にはパスワード管理が大切です。

竹内 ： 私は青色申告を e-Tax(電子申告)で行う為にカードを作りました。従来は青色申告をすると65万円まで特別控除があったのですが、今年の申告からは e-Tax なら65万円、従来通りの紙での申告は55万円と、10万円の差がつけられました。カードリーダーを購入しなければなりませんでしたが、こちらの方が得です。勿論、マイナポイントも貰いました。マイナンバーカードを作成する際、パスワードを3種類設定しなければならず、紙に書いて保管していますが、カードを持ち歩くことはしていません。

牛山 ： マイナンバーはそれ自体が唯一無二であるはずで、その活用システムをしっかり構築すべきであったと思います。偽造のしやすいカードを作ることで脆弱性が増し、セキュリティ対策がより必要になったのではないかと懸念しています。

司会 ： 今回はあまりなじみのない話題で、意見が出ないのではないかと心配していましたが、思いのほか多くのご意見を頂けたと感謝しております。いよいよ、プロセス安全もサイバー攻撃を考えないではいられない状況になってきたと実感しました。長時間に渡り、ありがとうございました。

キーワード: サイバーセキュリティ、サイバー攻撃 、計装システム、DCS、ランサムウェア、マルウェア、
安全計装システム、フィッシングメール、ネットワーク、ハードリレー、オープンアーキテクチャー
スクラッチ、ビスケット、JABEE、デジタル・トランスフォーメーション、マイナンバー、一方向ゲートウェイ

【談話室メンバー】

飯濱 慶、今出善久、牛山 啓、金原 聖、木村雄二、塩谷 寛、澁谷 徹、竹内 亮、春山 豊、林 和弘、
松井悦郎、三平忠宏、山岡龍介、山本一己、頼昭一郎

以 上