「制御システムセキュリティ──脅威と対策」特集号

解　説

次世代プロセスオートメーションとセキュリティ

橋本　芳宏*

1. はじめに

プロセスオートメーションは，シングルループ・コントローラにより，計器をみながら弁などを操作する単純労働から人間を解放して以来，より高精度に，より高速にと，生産効率の向上に貢献してきた．1975年には，横河電機がCENTUMを，ハネウエルがTDCS2000をそれぞれ独自に開発し，多くのシングルループ・コントローラがパネル上に配置されたパネル計装から，コンソール上の画面を切り替えながら運転管理をするDCS(Distributed Control System)による制御が広く普及してきた．それから40年以上たった2016年に，そのコンソールオペレーションを牽引してきたExxonMobilから，第1図のような次世代システムの提案が行われている[1].

サイバーセキュリティという観点から，プロセスオートメーションにイノベーションが起こるのは必至であり，DCSからこの構造へ変化する必然性と，そこでのセキュリティ対策の考え方について述べる．プラントオートメーションに対するセキュリティ対策の検討には，情報セキュリティの技術は必要であるが，守るべきプラントオートメーションシステムの設計・運用に当たるエンジニアが主体的になるべきであり，計装エンジニアがどのような観点でセキュリティを検討できるかを論じる．

2. コントロールシステムのセキュリティ対策の必要性

2010年にイランのウラン濃縮用の遠心分離機のコントロールシステムを対象にしたStuxnetが見つかって以来，インターネットに接続されていないコントローラでさえサイバー攻撃の標的になりうることがわかり，プラント計装へのサイバーセキュリティ対策の必要性が強く認識されるようになった．2015年には，通信の脆弱性をついて高速道路を走行中のジープのハンドルやブレーキを遠隔操作できることがわかり，クライスラーは140万台のリコールを余儀なくされた．同年12月にはウクライナで30か所の変電所がBlack Energy 3というマルウェアで同時に攻撃され，コールセンターも不能にされ広域での停電が発生した．2017年には日本でもWannaCryというマルウェアで多くの被害が発生したが，海外では病院や重要インフラに深刻な被害が出ている．そのため，次世代プラントオートメーションはサイバーセキュリティ対策がとりやすい構造でなければならない．

3. IoTの革新性と制御系の関係

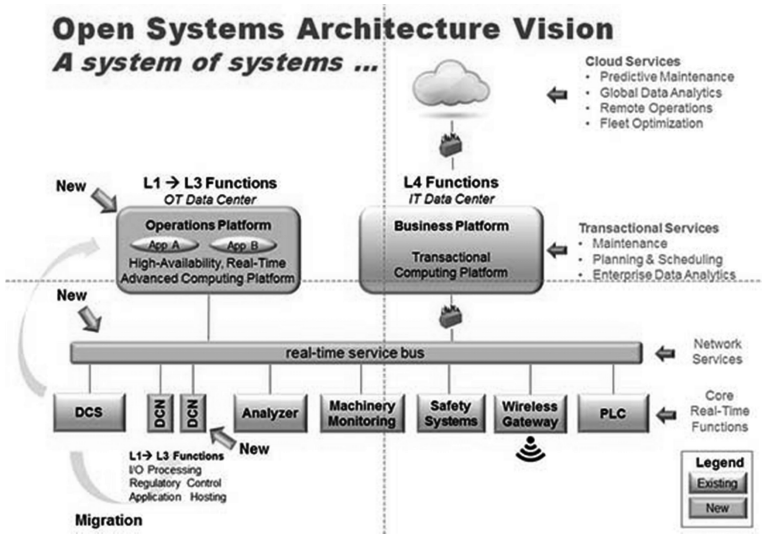
また，次世代プラントオートメーションは，情報化の動きを考慮したものでなければならない．世の中，IoT, AI, Big Data, Deep Learningという言葉が踊っており，とくに，ドイツではIndustrie 4.0，アメリカではIndustrial Internet Consortium，そして日本はSociety 5.0だといって，政府も大きな予算を拠出している．どの企業でも，本来なら，なんとかしなければならない経営者が，なんかしなければと社員を叱咤しているものの，目新しい成果は現れず，他所での成功例を求めてセミナーだけが盛況という事態を続けている．本来の革新性に目を向けた議論になっていないと感じられてしかたがないが，このIoTも次世代システムの必然性を示すものと考えられる．

まず，著者が考えるIoTの革新性について説明する．Industrie 4.0では第4の産業革命といっているが，Internet of Thingsであるので，「もの」についてイノベーションを考える．「もの」としての革新を第2図に示すように整理し，IoTは，単に通信でつながるのではなく，iPhoneのSiriのように，通信の先には，会話を実現するような「インテリジェンス」が存在することに注目する．「もの」と「インテリジェンス」が通信でつながることが，革新性を生むと考えるのである．

上記③のスマート化の代表例として電子炊飯ジャーを挙げて，④の革新性を考える．富士山の頂上にもっていくとうまく炊けなかったとすると，③でのカイゼンであれば，圧力センサを追加し，メモリを追加し，CPUを置き換えることになるだろう．④の観点では，通信機能が電子ジャーについていると，通信から位置がわかり，クラウドで気象庁等から圧力情報を得ることができる．クラウドにはCPU，メモリの制限がないので，そちらで圧力に応じた加熱法を演算し，炊飯ジャーには温度制御のパターンをおろせばよい．クラウドから指示するので，インターフェイスは，「もの」につける必要もなく，スマホからおばあちゃん用のごはんといえば，その好みの炊

* 名古屋工業大学

Key Words: cyber-security, next generation, process control, fog, diversity.



第 1 図 ExxonMobil から提案された次世代システム

第 2 図 IoT による「もの」の革新

き方を実現できる.「もの」自体はシンプルな機能をもっていれば，クラウドでいろいろな機能を追加できるのが,「つながる」価値で，インテリジェンスが「もの」の性能の乏しい CPU や容量の少ないメモリという「物理的制約から解放」される.

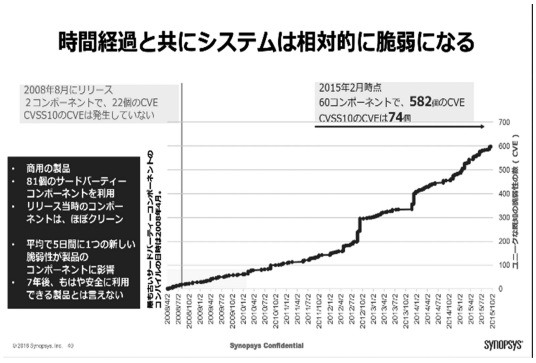
さらに，Google Map の渋滞情報も④の可能性を示すものと考えられる．ユーザは現在の場所の地図をさっと表示してもらいたくて，自分の GPS 情報を上げるのだが，GPS 情報が大量に集まるとその移動から渋滞を推定し，共通の地図に表示することで，渋滞を回避したい人の役に立てることができる．自動運転車は自分にどれだけセンサをつけても，ビルの陰から飛び出してくる自転車を検知できないが，自転車と同じ方向を走っている自動車がカメラなどで検知し，クラウドに知らせ，渋滞情報のように，将来の危険を共有できれば，事故を回避できるかもしれない．このように,「もの」から離れた「インテリジェンス」とつながることで,「もの」はどんどん高度化することができ，そこには物理的にも空間的にも，そして予測まで考えれば，時間的にも制約のない世界が広がると考えられる.

このような革新性をコントロールの世界でも考えると，DCS というハードウェアからコントロールというサービスを解放するというように，第 1 図の提案を読み解くことができる．DCN というコネクタの先には，センサ，アクチュエータや，単機能のコントローラを接続し,「インテリジェンス」は，Platform 側に置く．次章では，この Platform がどうあるべきかについて論じる.

4. セキュリティ管理

「もの」に「インテリジェンス」からの指示が通信で送られるときには，セキュリティへの配慮が必要である．**2** 章ですでに述べたように,「もの」を誤操作，誤動作させるサイバー攻撃は，現実のものになっている.

サイバー攻撃は，通信やアプリケーションの脆弱性をついてくる．この脆弱性は，セキュリティを意識せずにプログラム開発を行うから発生するというものではなく，いかに慎重に開発しても発生してしまう．第 3 図はアプリケーション・セキュリティ企業のシノプシスから入手した資料であるが，セキュア開発して 2008 年にリリースしたシステム（に用いているモジュール群）に見つかった脆弱性の数の推移を示している．CVSS10 はシステムを乗っ取られるような危険性の高い脆弱性で，7 年で 74 個も発生している.



第 3 図 セキュア開発したシステムの脆弱性の推移 [2]

アメリカの NIST の脆弱性データベースでは，2012 年以降，脆弱性が急増しており，現在，見つかっていなくても明日には見つかるかもしれないと考えなければなら

10年前に社員が開発したプログラムに、利用されている
モジュールに脆弱性が見つかったと報告を受けた。

セキュア通信のモジュールOpenSSLの脆弱性が報告されることもある。

- だれが、プログラムの修正をする？
  - その社員の現在の仕事は？
  - 他の人に頼めるプログラム修正？
- モジュールの修正版はいつ入手できるの？
  - それまで、プラントは停止するの？
- そのモジュールの修正パッチが入手できたとして
  - 10年前のCPU,メモリで適用できるの？
  - リアルタイム処理に悪影響しないか、テストするには？
- そのモジュールを利用しているプログラムは社内に他にないの？

第 4 図　セキュリティ管理の課題の一例

ない．脆弱性は，開発時だけでなく，運用時にも配慮し続ける必要がある．

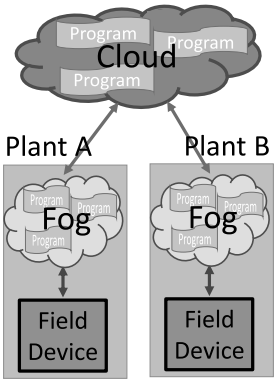
製造現場にはコントローラだけでなく，SCADA, 生産管理，設備管理など多くのシステムが存在するが，すべてのプログラムはセキュリティホールになる可能性がある．サイバー攻撃も安全破綻の重要な要素であると考えると，脆弱性管理は安全担保のために必要である．

大量のプログラムの脆弱性をどのように管理すべきなのであろうか．プログラムは現在，オリジナルなコーディングを避けて，既存のモジュールをできるだけ利用して開発する．そのため，ソースコードがなくても，バイナリのパターンから使用されているモジュールを推測できれば，前述の NIST CVE Database で脆弱性を知ることができる．すでに，ソフトウェアの脆弱性管理を製造業の BOM のようにモジュール単位で行えるツールも存在する．そのようなツールを利用して脆弱性の所在がわかったとして，どのように対応することになろうか．

第 4 図に脆弱性検知後の問題の一端を示す．10 年前の CPU とメモリではパッチがあてられない可能性が高いし，あたっても遅くなって使えないことになるかもしれない．IoT といって性能の乏しい CPU と容量の少ないメモリでスマート化を図ると，すぐに同様の問題が発生することにも気づいていただけると思う．IoT でもセキュアな通信は維持し続けることが求められるので, 通信機能に将来発生するかもしれない脆弱性に対応できるだけのハードの余裕と通信による更新機能は必要であると考える．

5. クラウドによるプログラム管理を制御にも

脆弱性の発生は回避できないものであり，故障のように予備品との交換で，すぐに対応できるものでもない．事務系ではすでに社員の PC はブラウザのみにし，アプリはサーバで管理するシンクライアント化が進んでいる．また，サーバもクラウドで実現することが一般的になっており，大地震が発生しても，サービスは継続できるし，必要な容量だけの出資で済み，セキュリティの管理もやってもらえる．クラウド側は，サーバを多くのユーザに共同利用してもらうことで稼働率を高めることができるし，多くのサーバを所有することで，フレキシブルな運用が可能になる．



第 5 図　Fog による制御

クラウドでも脆弱性は発生するが，複数のサーバが存在すれば，切り替えながらパッチあてなどの対応を，サービスを継続しながら行うことが可能である．

コントロールというサービスの「インテリジェンス」の部分をクラウドで実現すれば，プログラムの脆弱性に柔軟に対応できる可能性が生じる．

しかし，コントロールはプラントの安全にも必要な機能で，どこにあるかわからないサーバに命は預けられないと通常考えると思われる．そのため，事業所内に，コントロールというサービスを提供するローカルクラウドを置くことを考える．場所は，自分のところにあるが，複数のサーバで，どれがサービスを提供しているかは，シングルループ・コントローラなどのフィールドデバイスは知らなくてもよいという特性をもつクラウドなので，フォグとよぶ．クラウドと異なり，サーバが事業所に存在することになるので，資産管理の面で，できるだけ簡素になることが望まれる．そのため，第 5 図に示すように，リアルタイム性が要求される機能だけフォグで実行し，リアルタイム性の低い機能は，クラウド内のアプリとして実現されると考えられる．

第 1 図の ExxonMobil の Platform の提案にはこのフォグの概念までは表明されていないが，リアルタイム性を強調しているのでフォグに対応するものと考えられる．

フォグはフィールド側へはリアルタイムのサービスを要求されるが，脆弱性に対するパッチあてなどの対応は，すぐにできるものではない．インテリジェンスをフォグとクラウドに集中させることにより，脆弱性への対応はセキュリティ・スペシャリストが遠隔から行うという体制が可能になる．高まり続ける脆弱性の発現頻度に対応しきれるセキュリティ・スペシャリストを，すべての事業所で確保できるとは考えられず，フィールドに「インテリジェンス」を置かないクラウド，フォグ，フィールドというコントロールシステムの構成は必須のものとなると考える．

6. クラウド，フォグ，フィールドの階層システムに対するセキュリティ対策に求められる多様性

プラントの安全を考えた場合，サイバー攻撃でプラントに変化が現れるのは，コントローラ，アクチュエータの誤動作，不動作，あるいは，センサ値を改竄されたことによる誤操作に限られる．つまり，サイバー攻撃による「悪意の誤動作，誤操作」の可能性を解析し，対策すれば，サイバーセキュリティ対策になる．

安全解析では，誤動作，誤操作はすでに検討されているはずで，安全解析で洗い出せなかった事故が，サイバー攻撃で発生するわけはなく，発生確率の評価が，従来の安全解析と異なるものになるだけである．

サイバー攻撃に対する防御は，ルールなき戦いであり，想定外の手口での攻撃を前提に検討しなければならない．そして，脆弱性は，いつ発生するかわからず，すぐには対策をとれず，脆弱性が存在する状態を想定しなければならない．

その前提で，コントローラの誤動作，誤操作を防ぐためには，コントローラまでのパスを多重多層に防御策を用意することになる．制御システムのサイバーセキュリティに関する世界標準である IEC 62443 でも，Zone & Conduit によるセキュリティ対策と評価が推奨されている．これは，工場の正門に守衛を置き，建物の玄関，窓，部屋の扉に鍵を設定し，構内および廊下，部屋内に防犯カメラを設置するという通行の管理・制限・監視に相当する．しかし，その標準にも記述されていない最も重要な特性は多様性である．多重多層でも鍵が同じであれば，全滅する．弱点が異なる防御の組合せでなければ，未知の攻撃には対策になりえない．効率を重視すれば，共通部品になり一人勝ちの世界につながってきたが，セキュリティを考えると，それは全滅の危険性の高い戦略となり，多様性が重視される生態系本来の特性と共通になる．最も良いものが生き残るのであれば，オスとメスに分かれる必要はないし，自分が生き残ることを重視するときにイワシは大群を構成するであろうか．

フォグの中に存在する切り替え候補は，異質でかつ同じ機能を発揮するものであるから，未知の脆弱性への対策になりうるのであり，同じものならいくつ並べても全滅してしまう．セキュリティを重視すると，一人勝ちの格差拡大の世界ではなく，多様性を尊重した優しい世界になると期待できる．

7. フォグとフィールド間のセキュリティ対策

プラント安全へのサイバーセキュリティの脅威に関しては，前述のように，コントローラの誤動作，誤操作として扱えるので，コントローラをインターフェイスとした解析を行えば，サイバー攻撃の手口が未知であろうと，システマティックな対策検討が可能になると期待できる．フィールドデバイスは，シングルループ・コントローラかセンサ，アクチュエータであるとし，それらにサイバー攻撃が及んでしまっても，安全を守ろうと考えると，まず思いつくのは，物理的な防御との組合せである．

7.1 物理的な防御との組合せ

サイバー攻撃は情報操作によるものなので，手動弁や手動スイッチ，リレー回路を操作することはできない．オーバーヒートをサーモスタットの回路で防御しているヒータをサイバー攻撃でオーバーヒートさせることはできない．空焚き事故であれば，液位が空にならない制御かヒータを加熱し続けない制御のどちらかを物理的なものにすれば，サイバー攻撃での事故発生を防ぐことができる．すべてを論理回路で組まなくても，一部を物理的な信号で動くシステムにして，通常のコントロールシステムと組み合わせることで，たとえサイバー攻撃がコントローラに及んだとしても，安全を確保できる可能性が生じる．いかに簡便でサイバー攻撃に対して効果のある組合せを設計するかは，計装エンジニアの問題である．

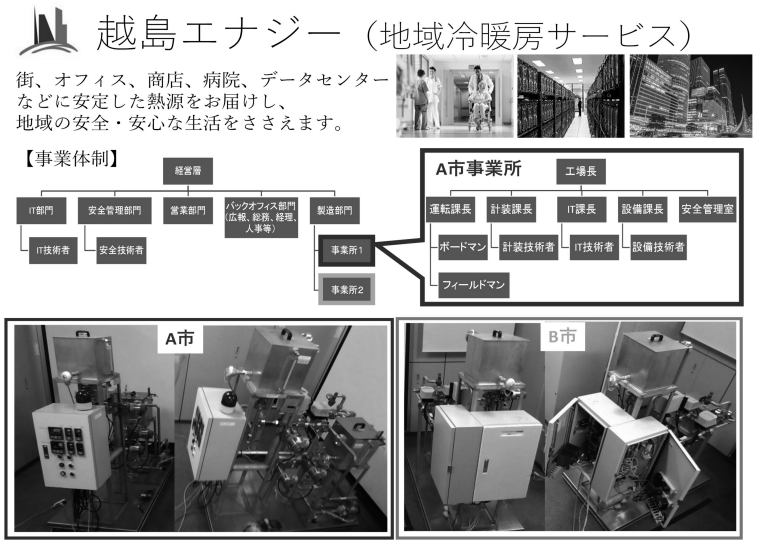
7.2 コントローラ群のゾーン分割

コントローラは安全や品質のために機能しているものなので，サイバー攻撃ですべてのコントローラが敵の手中に落ちてしまうと，停止させることはもとより事故を発生させることもできる．サイバー攻撃が及んだとしても，すべてが陥落しないように，一部は生き残って安全を確保できるように，コントローラ群を複数のゾーンに分割することもセキュリティ対策である．第 1 図のリアルタイム・サービス・バスというネットワークは一つのように書かれているが，セキュリティだけでなく故障を考えても複数個が並列に用意されると考えられる．そのネットワークとフォグの接点には異なるゲートウェイを設置し，ネットワークとフィールドデバイスの接点にも異なるコネクタを利用することで，脆弱性の発生が通信経路ごとに異なるように設定することも可能である．

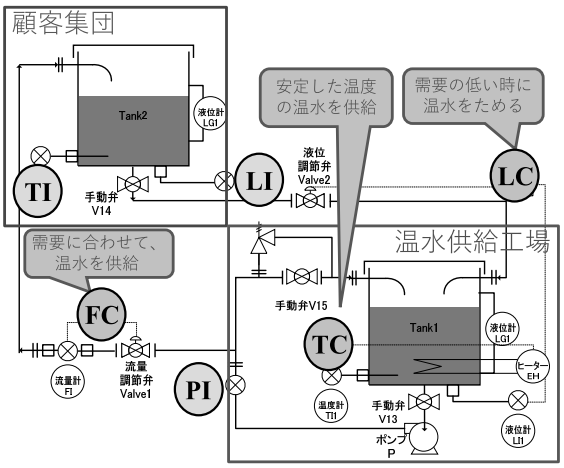
そのうえで，フィールドデバイスであるコントローラ群を異なるネットワークに振り分けて接続することで，コントローラが全滅する危険性を抑制する．この振り分けをゾーン分割とよぶ [3,4]．つぎに，コントローラ群のゾーン分割の設計法を解説する．

7.3 セキュリティに注目した安全解析

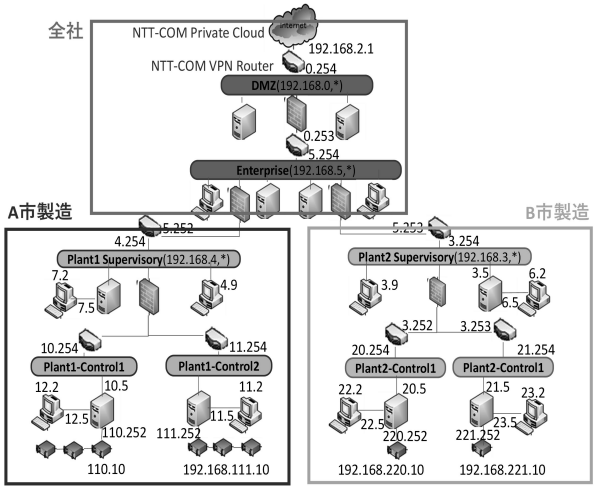
産業システムのコントロールシステムは設計時に安全解析が行われ，FTA による事故の発生確率の算出が行われている場合もある．サイバー攻撃は悪意によるものであるので，これでもかと攻撃をたたみかけてくる可能性がある．危険な状態にする操作を行ってもすぐに被害が発生するわけではなく，近年，化学プラントで連発した人身事故では，トリガーが発生してから事故に進展するまで半日以上かかったものがあるので，危険にする操作に気づかせないようにする隠蔽工作も同時に行い，事



第 6 図　仮想企業「越島エナジー」とプラント

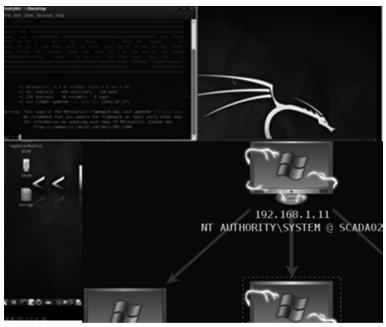


第 7 図　プラントの構成



第 8 図　ネットワーク構成図

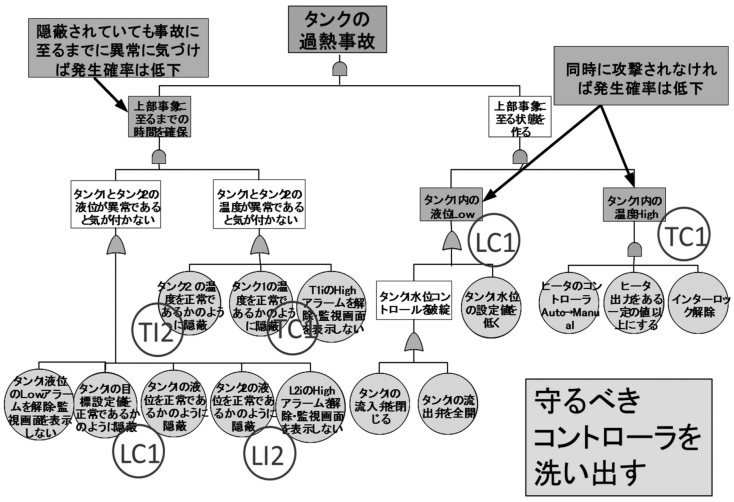
故を確実に引き起こそうとすると考えられる．そのため，サイバー攻撃による事故発生の危険性を解析するためには，事故を発生させる状態をつくる困難さとともに，気づかれないように情報を改竄する難しさも考慮する必要がある．そのための FTA を筆者らは提案している [5] が，抽象的な議論ではイメージを共有しにくいので，以下に示す具体的な対象を用いて，安全解析および対策を解説する．



第 9 図　Metasploit を利用したハッキングデモ

8.　セキュリティ対策検討のための仮想企業

われわれの研究室では，企業規模でのさまざまなセキュリティ対策を検討するため，第 6 図の写真に示す 2 台の温水循環プラントを用いて，二つの地域に対する地域暖房サービスを行う仮想企業を作成している．第 7 図に温水循環プラントの構成を示すが，ヒータ付きのタンクが工場で，もう一つのタンクが温水を供給される顧客群をまとめて表したものとみなす．顧客の需要に応じて，安定した温度の温水を供給する制御が働き，工場の液位制御の目標値は日内変化するとしている．第 8 図に企業体のネットワーク図を示すが，温水供給工場と顧客群の状態を監視する SCADA がそれぞれ存在し，さらにそれらを統括監視する SCADA が各事業所にあるという構造をとっている．さらに，それらの操業用ネットワークが，全社的な調達や販売，生産計画，設備管理などを行う業務系ネットワークに接続され，その業務系ネットワーク



第 10 図　サイバー攻撃による事故の FTA

は，DMZ を通じてインターネットに接続される．

プラントの計装は，市販の工業計装を用いたもので，SCADA を含め，上位ネットワークは，VMware を用いた仮想環境の上で構築しており，各サーバや PC の OS やアプリは，複数組用意しており，ネットワーク構成も柔軟に切り替えられる．

監視カメラを含めすべての通信を OPC-UA に限り，最新の OS とアプリを用いて，セキュアな設定をしたうえに，セキュリティベンダーの最新ツールを満載した構成も実現できるし，OS に Windows XP を利用し，Firewall などを設定せず，OPC-DA を用いて，脆弱性たっぷりな構成にもできる．

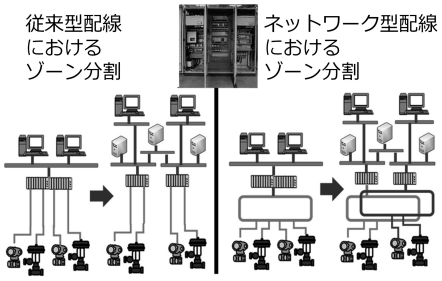
第 9 図に示すような一般にダウンロードできるツールでパスワードも不要で簡単にハッキングでき，ちょっとスクリプトを作成すれば，プラントを危険な状態にして，かつ，それを SCADA 画面には現わせないというサイバー攻撃も，いとも簡単にできてしまうというデモも行っている．

内閣府の戦略的イノベーションプログラム (SIP) や経済産業省の ICS-CoE において，重要インフラを主とした産業システムのサイバーセキュリティを向上させるための人材育成にも関係しており，インシデントレスポンスの演習にも，この仮想企業を利用している．

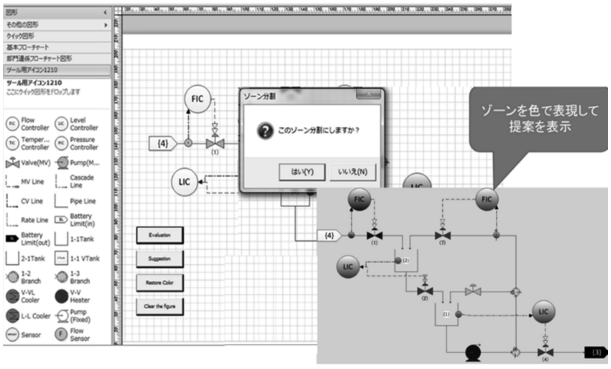
さらに，主要セキュリティベンダー，計装ベンダーが集い，最新ツールを持ち寄り，この仮想企業に実装し，実際に，高度なハッカーがサイバー攻撃を行うという「つるまいプロジェクト」も進行している．ネットワークの検知システムを，プラントオペレータが活用するための出力方法や利用方法を検討したり，ベンダーの垣根を越えて，セキュリティ対策を普及するための提案方法を検討している．

9. リスク解析例

7.3 で解説したサイバー攻撃に対する安全解析の例を第 10 図に示す．



第 11 図　ゾーン分割のための変更



第 12 図　隠蔽工作を防ぐゾーン分割設計用 CAD

この FTA の特徴は，まず，操作の条件と隠蔽の条件に分岐する点にある．そして，通常の安全解析であれば，腐食や疲労破壊なども原因に解析されるであろうが，サイバー攻撃は，コントローラを通じた操作か，センサを改竄することで引き起こす誤操作に，プラント変化の原因は限られるので，コントローラ異常か，センサ異常が現れると，それ以下の解析は行わない．そして，AND 条件に現れるコントローラやセンサは，どちらかが生き残れば，事故にはならないことを示すので，別のネットワークに配置し，それぞれのネットワークの防護に異なる種類の防御策を施すようにする．

第 10 図の例では，二つのタンクのレベルセンサを別のゾーンにすれば，片方が生き残れば，生き残ったセンサで変化に気づくことができ，工場の液位制御と温度制御を別のゾーンにすれば，空焚きを防ぐことができることを示している．

従来はひとまとまりに扱われていたコントローラの配線を，第 11 図のように別のネットワークに分割することになるが，その変化は計装のラック内の変化でほぼ済み，それほど管理が複雑になるわけではない．

化学工学会システム・情報・シミュレーション部会プラントオペレーション分科会のアンケート調査では，一人のオペレータが担当するコントローラが 1000 を超える例も少なくない．大量のコントローラのゾーン分割を検討するのはたいへんな労苦になると考えられるので，われわれの研究室では，隠蔽工作を回避するためのゾーン分割案を提案する CAD（第 12 図参照）と，AND 条件のコントローラの組を洗い出すための FTA の CAD を，Microsoft VISIO を利用して開発している [6].

10. おわりに

本稿では，プロセスオートメーションが変革の時期であり，サイバーセキュリティが信頼性の評価の重要な要素となると，システムの構成と管理が変化していくはずであるという論理を展開した．脆弱性はいつ発生しても不思議ではなく，サイバー攻撃では想定外がつきもので，これでもかと同時多重に襲ってくるという前提で，サイバーセキュリティを考えるとき，守るべき「もの」に基づいた検討をせざるを得ず，「もの」とのインターフェイスは，コントローラであるので，制御技術者が主体になって対策を検討すべきである．この観点で，制御技術者が検討できる対策の一部を紹介した．

まだまだ，制御系のサイバーセキュリティ技術には課題が多く，今後，制御やシステムを専門にする技術者がセキュリティに積極的に取り組んでいただけることを期待している．

(2017 年 9 月 29 日受付)

参 考 文 献

[1] B. Lydon: ExxonMobil to build next generation multi-vendor automation architecture (2016); https://www.automation.com/automation-news/article/exxonmobil-to-build-next-generation-multi-vendor-automation-architecture (2016.2.16)

[2] 明石: シノプシス ソフトウェア インテグリティ グループご紹介, SIG4Overview_20170721.pdf (2017)

[3] Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, S. Jing and I. Koshijima: Conceptual framework for security hazard management in critical infrastructures; *The 11th International Symposium on Process Systems Engineering* (2012)

[4] Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, S. Jing and I. Koshijima: Safety securing approach against cyber-attacks for process control system; *Computers & Chemical Engineering*, Vol. 57, pp. 181–186 (2013)

[5] 豊嶌, 孫, 越島, 橋本: サイバーテロを想定した場合のリスク解析と対策の構築; *J. of Human Factors in Japan*, Vol. 15, No. 2, pp. 4–9 (2011)

[6] H. Moritani, S. Yogo, T. Morita, M. Kojima, K. Watanabe, J. Sun, I. Koshijima and Y. Hashimoto: Development of CAD for zone dividing of process control networks to improve cyber security; *ICCAS 2014* (2014)

著 者 略 歴

橋本（はしもと） 芳宏（よしひろ）

1957 年 12 月 1 日生．1985 年 3 月京都大学大学院工学研究科化学工学専攻博士課程単位取得退学．同年 4 月名古屋工業大学助手，2003 年 4 月同大学教授となり現在に至る．プロセスシステム工学，プロセス制御，障碍者支援などの研究に従事．計測自動制御学会，化学工学会などの会員．