特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

# 4 化学プラントのサイバーセキュリティ
## ―OT システムのセキュリティ脅威に対する取り組みと今後の展望―

応用 一般

星野浩志　秋元新哉
横河電機（株）

## 化学プラントに対するサイバーセキュリティ脅威の進化

ガートナーグループが公開した今後数年間のサイバーセキュリティに関する動向を予想した記事[1]の中では，2025 年までにマルウェアによるサイバー攻撃によって OT[☆1] 環境が兵器化し，人的被害が発生することを予想している．同社は，サイバー攻撃の影響がビジネスの混乱から人的な被害へとシフトし，最高経営責任者（CEO）の責任が問われる可能性に言及している．このような状況が現実化することは想像したくないが，ここ数年のサイバー攻撃者の OT 領域の知識の深化と，OT システムへのサイバーセキュリティ攻撃による社会生活への影響の発生事例を見ると，化学・石油プラント（図 -1）を取り巻くサイバーセキュリティ脅威は確実に進化していると言える．

化学・石油プラントに対するサイバーセキュリティ脅威が現実化した事例を 2 つ挙げる．2017 年にサウジアラビアで発生した石油化学プラントへのサイバー攻撃によるプラントシャットダウンがある．この事例では，プラントの緊急時自動停止を行う安全計装の専用コントローラへのマルウェア（TRITON）の感染が，プラントシャットダウンの原因であると特定されている．このマルウェアの開発には専用の組込み機器内部の設計・実装に関する深い知識を必要とすることが分かっている．攻撃者の真の意図はいまだに不明であるが，もしプラントが緊急時に安全に制御できない事態に陥っていたとしたら，人命や安全にかかわる問題に発展した可能性があった．

2021 年 5 月に発生した米国最大の石油パイプライン事業者である Colonial Pipeline 社へのランサムウェア攻撃の事例では，パイプラインが 6 日間の操業停止に追い込まれたことで，ガソリン供給不足の懸念から社会的混乱が発生した．この事態を受けて同社 CEO が米国上院国土安全保障・政府問題委員会で説明を求められた．Colonial Pipeline のインシデント事例で注目すべき点は，IT 環境側のインシデントが OT 環境側に影響を及ぼす前の段階で OT 側のシス

☆1 Operational Technology（OT）とは，産業用機器，資産，プロセス，イベントなどを直接監視・制御し，変化を検知・誘発するハードウェアとソフトウェアのこと（Gartner による定義）．

■図 -1　化学・石油プラント

テムを自ら停止したことである．しかもこの対応は，あらかじめインシデント対応プロセスとして定められていたという．OT 側のシステムを停止したのは料金請求システムが侵害されたためであるという報道もあり，業態によっては IT と OT のシステムの区分が難しい可能性があることが認識された事例である．

今後 OT ネットワークがさまざまなものとつながることでさらにサイバーセキュリティ脅威が進化し，社会的影響が生じる可能性が高まることが予想される．このような事態に継続的に対応していくためには，OT 分野のシステム・機器の知見や運用現場の人・プロセス・技術の知見と，IT 分野の知見の両方が必要になる．そこで本稿では，IT 分野の読者に向けて，化学プラントの OT システムである生産制御システムのサイバーセキュリティ関連の動向および課題と今後の展望について紹介する．

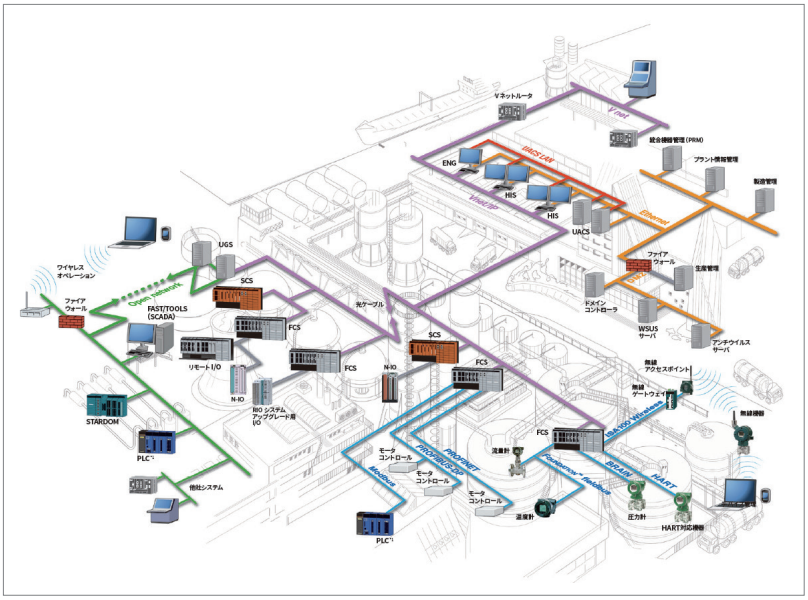
## 化学プラントの特徴とサイバーセキュリティの取り組み

化学プラントは自動車の組み立て工場などと異なり液体や気体を製造するもので，その多くが危険物質である．エチレンなどの基礎化学品の大量製造プラントから，素材に特殊な機能を持たせた高機能性化学品製造プラントまで化学プラントの姿は多様である．さらに石油化学・ガスまで範囲を広げると，石油精製プラント，油井，LNG（液化天然ガス）処理プラントおよび輸送用パイプラインなど幅広い．これらのプラントの自動制御[☆2]を行う生産制御システムには，以下のような特徴がある．

①広域に運用される多様な機器
② 20 年もの長期にわたる機器運用・保守
③リアルタイム制御
④無停止連続監視・制御

ここで言う機器には，広い工場の敷地に配置されたタンクや配管などの設備に取り付けられた温度・圧力等のセンサやバルブ，これらの PID 制御を行う分散制御システム（DCS）（図 -2），数千キロメートルにわたるパイプラインを監視する SCADA[☆3] システムがある．一般的な IT システムとの違いとしてよく強調される②③④には，プラントの運用において人命・安全・環境・品質への最大限の配慮が求められることが背景にある．

1970 年代から 1980 年代頃の化学プラントの生産制御システムでは，ベンダ独自のハードウェアと通信プロトコルを利用していた．1990 年代から 2000 年代にオフィス側の IT システムとのデータ交換やコストダウンの必要性から UNIX，Windows といった汎用 OS の活用や，制御通信への TCP/IP 等の汎用通信プロトコルの活用が進んだ．オペレータ用操作監視インタフェースやエンジニアリングワークステーションなどその実体は IT システムと変わらないものになり，その結果 IT システムと同様のサイ




■図 -2　工場内に設置されたセンサ・バルブ・分散制御システム（DCS）の例（横河電機 統合生産制御システム CENTUM VP カタログより）

☆2 「プロセス制御」や「プロセスオートメーション」という用語が使われる．
☆3 Supervisory Control and Data Acquisition

バーセキュリティ脅威にさらされるという状況に直面した．一方，前述の生産制御システムの特徴から，OS やアプリケーションのセキュリティパッチを頻繁に適用するような，IT システムで一般的に行われているセキュリティ対策の実施が困難な状況も見られた．その後 2000 年代に，米国で国土安全保障が喫緊の課題となったことから，重要インフラの防衛に関する問題意識が高まった．化学プラントにおいてもサイバーセキュリティ強化の機運が高まり，石油化学業界の主要企業等がプラントの生産制御システムに対するセキュリティ対策のベストプラクティスの収集や，セキュリティ技術対策・運用対策の標準化，人材育成に取り組むようになった．生産制御システムのセキュリティ対策・運用の国際標準規格である ISA/IEC 62443 シリーズはこれらの取り組みの成果の 1 つであり，IT 分野における情報セキュリティの国際標準規格である ISO/IEC 27000 シリーズや ISO/IEC 15408 に対比されるものである．現在 ISA/IEC 62443 は化学・石油・ガス事業者から生産制御システムのシステムインテグレータ，サービスプロバイダ，制御機器プロバイダまで広く参照・活用されており，さらに自動車工場，ビルオートメーションや鉄道等の分野で活用が広がっている．

## スマートファクトリーの進展と制御システムセキュリティ

2010 年代後半になると，デジタル技術やクラウド技術の活用によって生産業務プロセスの改革や生産性・品質の向上を継続的に行うスマートファクトリーの実現を目指した取り組みが始まった．化学プラントでも，従来の PID 制御対象であるバルブや流量計だけではなく，さまざまなセンシング機能を持つ IoT 機器やロボット，ウェアラブルデバイスなどを使って，データを収集・分析したり，業務改善に活用したりする取り組みが進んでいる．この取り組みをさらに進めるために，生産制御システムのアーキテクチャをよりオープンで標準化されたものにする活動が始まった．この取り組み事例として，NAMUR Open Architecture（NOA）と Open Process Automation（OPA）の取り組み，およびセキュリティ対策の考え方を紹介する．

### NAMUR Open Architecture（NOA）

NOA[2] は，欧州の化学メーカを中心とした団体である NAMUR が提唱する，生産制御システムのオープンアーキテクチャである．従来の生産制御システムの構造や利点に影響を与えることなく，新たに導入する IoT に組み込んだセンサ等を活用し，プラントの監視および生産の最適化を簡単かつ安全に行うことを目的としている．

NOA では既設の生産制御システムである CPC（Core Process Control）の外側に M+O（Monitoring and Optimization）と呼ばれる独立したドメインを付け加えている（図 -3）．M+O にはプラントごとの M+O（Plant Specific M+O）および各プラントを統合管理監視するために設置された中央の M+O（Central M+O）がある．プラントごとの M+O にある新しいセンサ（たとえば，振動，音響，腐食，匂いなど）やロボット，ドローンおよび既設システムからデータを収集し，M+O ドメイン内でこれらのデータを元に高度な制御，解析，診断を実現できることを目指している．

ドメイン間の通信は国際標準規格である OPC UA を採用し，さまざまな機器がセキュリティを確保しながらプラントごとの M+O に接続できるようにしている．NOA では ISA/IEC 62443 が提唱するゾーン分割の考え方を取り入れ，各ゾーンすなわちドメインごとに想定するセキュリティ対策のレベルを定めた上で，各ドメイン境界において必要なセキュリティ対策を取ることを求めている．具体的には M+O と CPC の間のデータ通信を，一方向のフローのみを許可するセキュリティゲートウェイによって制限する．これは特に安全面から重要な設備である CPC を，そ

れ以外のドメインから保護することを目的としている．またセキュリティゲートウェイおよび各ドメイン内の個々の機器については，ISA/IEC 62443 のコンポーネントに対するセキュリティ要求に基づいて，ユーザ認証・マルウェア対策・ログ機能等の必要なセキュリティ対策を実現することを求めている．

## Open Process Automation（OPA）

OPA は石油化学大手事業者を中心とした団体である Open Process Automation Forum（OPAF）[3] が提唱する，新しい生産制御システムのアーキテクチャである．OPAF には，石油化学，医薬，紙パルプなどのさまざまな業種から，ユーザ企業，システムインテグレータ，ソリューションプロバイダなど約 130 の企業・団体が参加している．日本からは横河電機もこの活動に当初より積極的に参加しており，システムインテグレータとして石油化学事業者向けのテストベッド構築を担当するなどしている．

OPA のねらいは，標準に基づいた，オープンかつセキュアで相互運用可能な生産制御システムのアーキテクチャを構築することである．OPA では生産制御システムを構成するためのコンポーネントを柔軟に組み合わせたり置き換えたりすることが可能になる．これにより複数のサプライアが提供する製品の中から最適な（best-in-class）コンポーネントや最新技術を導入するなど，システム更新が容易になる．

そのベースとなるのが，OPAF が標準化を進めている O-PAS（Open Process Automation Standard）である（図 -4）．O-PAS ではハードウェアやソフトウェアなどのコンポーネント間のインタフェースを標準化することで，マルチベンダ間で相互運用が可能となる．OT 分野だけでなく IT 分野からも生産制御システム・機器への参入が進み，新たなイノベーションや付加価値のあるソリューション・サービスの提供が促進されることも期待される．

OPAF では，生産制御用機器の設計段階からインテグレーションされたかたち（Secure-by-Design）でセキュリティを浸透させることを目指している．これは，後付けでのセキュリティ対策が複雑かつ高コストになりがちであるという課題を解決するた

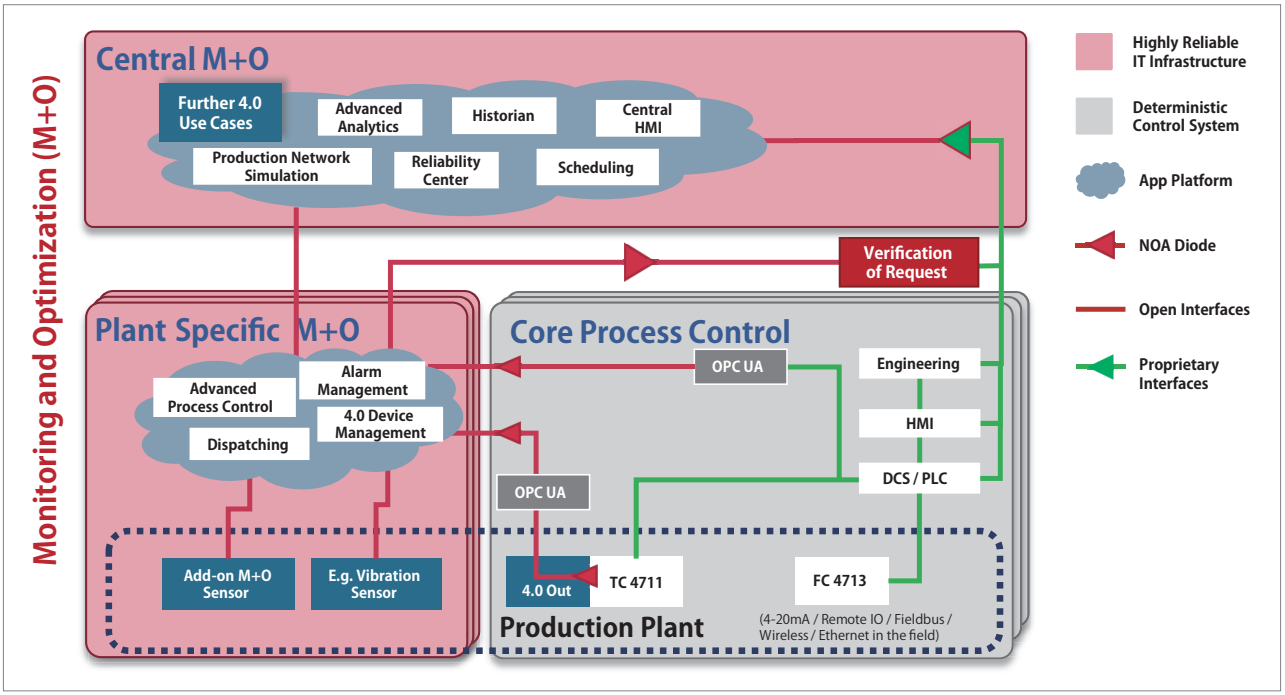
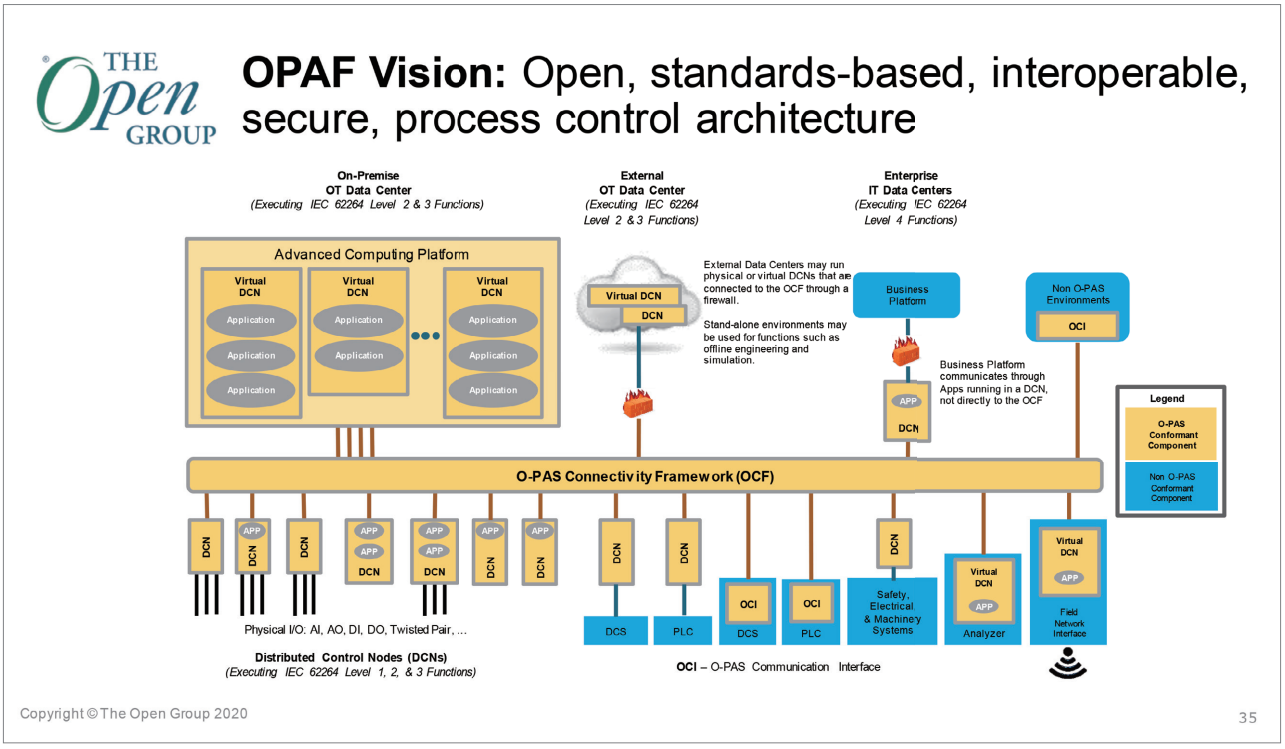



図 -3　NAMUR Open Architecture（NE 175:2020 NAMUR Open Architecture – NOA Concept より引用）

めの取り組みである．O-PAS では前述の NOA と同様にサイバーセキュリティのフレームワークとして，国際標準である ISA/IEC 62443 をリファレンススタンダードとして採用しており，各制御機器のセキュリティ要件とセキュアな制御機器開発ライフサイクルが標準化されている．各ノード間の通信およびデータの情報モデルについても国際標準規格である OPC UA を採用し，セキュアなデータ交換を実現している．これにより制御機器サプライアから一貫性のあるセキュリティ機能を備えた O-PAS に準拠した制御機器が提供されるようになり，サイバーセキュリティに強い生産制御システムの基盤となる．化学プラント事業者は，事業に適したセキュリレベルと必要なセキュリティ要件を決定し，システムインテグレータはエンドユーザの機能・セキュリティ要件を満たすべく生産制御システムの構築を行うことが可能となる．

## 課題と今後の展望 - IT と OT で求められること

化学プラント業界においても他の製造業と同様に，生産効率向上の追求やプラント運用管理の人員不足への対応が求められている．このような背景から，プラントから得られるさまざまなデータの生産現場における活用や，リモートアクセスの活用，現場の作業員の支援のためのデバイスの導入などが進展し，スマートファクトリーの実現に向かう．このような環境においては，従来の生産制御システムで一定の効果を発揮した境界防御型のセキュリティ対策はいずれ限界を迎える可能性がある．このようなことを想定して，境界内外を問わずすべてのサイバーセキュリティ脅威から制御機器や制御機能・データをきめ細かく守るためのゼロトラストセキュリティ対策などの新しい技術も常に視野に入れて取り組む必要がある．ただし，化学プラントの生産制御システムの長期にわたる機器運用の状況から見て，すぐにすべ




■図 -4　OPAF Vision（ARC Industry Forum 2021 より引用）

てを実現できるものではないため，現実に即して境界防御も含めた多層防御対策と，運用体制の構築・維持，事業継続計画立案が必要となる．これを実現するための国際標準や技術対策はすでに存在している．化学プラント事業者には，制御機器プロバイダ・システムインテグレータとともにセキュリティ脅威・対策技術の進展について知見を共有し，プラントオペレーションへの影響を最小におさえつつ，段階的に新しいセキュリティ対策を取り込んでいく取り組みが求められる．この取り組みを推進するためには，化学プラントの自動制御の根幹である OT システムにおける機器の設計・実装，システム構築，サービス提供の分野に，IT の知見を組み込んでいくことが必要になる．今後この分野にはさらに IT の知見を持つ人材が必要になる．

IT と OT の関係については，IT-OT Convergence によってプラント事業者内の IT，OT 部門の組織・技術のすべてを 1 つに集約すべきであるという意見がある．OT の世界に IT の知見が必要であることは間違いない．一方で前述の通り化学プラントの生産制御システムには一般的な IT システムとは異なる特徴があり，IT 用のセキュリティ対策ツールをそのまま導入すればよいわけではない．たとえばプラントの現場において，IT 用ツールのアラームメッセージを，人命やプラントの安全にかかわるものと同列に扱って良いかの判断は非常に難しい．

IT と OT のそれぞれの特徴や組織・文化の違いをふまえて，1 つの企業の中で統制のとれた効果的なセキュリティ対策を行うためには，IT と OT の組織・技術を 1 つに集約するのではなく，IT と OT の組織がそれぞれ独立した上で，経営層のリーダシップのもとに連携していくことが必要となる．現在，ISA/IEC 62443 の原案を作成している ISA99[4] において，プラントを運用する事業者企業のセキュリティリスクマネジメント体制の中で，IT と OT それぞれのエリアで個別に適切なセキュリティ対策をしつつ，共通のフレームワークを活用する方針が提唱されている．具体的には 1 つの企業の中で IT，OT を含めた ISO/IEC 27001，27002（ISMS）に基づくセキュリティ管理体制を構築した上で，IT エリアに対しては ISO/IEC 27001，27002 に基づくセキュリティ管理策を導入し，OT エリアに対しては ISO/IEC 27001，27002 と ISA/IEC 62443 の中から OT の生産制御システムの特徴をふまえたセキュリティ管理策を導入するというものである．将来的にこのような取り組みが実際の企業活動の中で行われることで，化学プラントに対してより効果的なセキュリティ対策が導入される体制が構築されることを期待して，本稿の締めくくりとする．

**参考文献**

1）The Top 8 Cybersecurity Predictions for 2021-2022, https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
2）NAMUR Open Architecture, https://www.namur.net/en/focus-topics/namur-open-architecture.html
3）OPAF（Open Process Automation™ Forum）, https://www.opengroup.org/forum/open-process-automation-forum
4）ISA99, https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

（2021 年 12 月 28 日受付）

■星野浩志　Hiroshi.Hoshino@yokogawa.com

1992 年東京農工大学大学院工学研究科電子情報工学専攻修了，同年横河電機（株）入社．社内 PSIRT 体制構築等を経て，制御システムのセキュリティ対策の提案と国際標準化活動に従事．CSSC 評価認証・標準化委員会委員．IEC/TC 65/WG 10 国内委員会幹事．

■秋元新哉　Shin-ya.Akimoto@yokogawa.com

2008 年慶應義塾大学理工学研究科基礎理工学専攻修士課程修了，同年横河電機（株）入社．製造業向けソフトウェア開発等を経て，石油化学大手向け OPA テストベッドの立ち上げ，サイバーセキュリティ・IT 基盤ソリューションの開発に従事．