プラントのサイバーセキュリティ動向とコントラクターとしての対応

Plant cyber security trend and countermeasure as a Contractor

濱田 佑希[*1]　太田 結隆[*2]

Yuki HAMADA　Yuitaka OTA

*1 プロジェクトマネジメント部プロジェクトコントロールセクション
Project Controls Sec., Project Management Department

*2 制御システム設計部
Control System Engineering Department

****

Abstract

Industrial Control System (ICS) of a plant is widely used in essential infrastructure (Power, Oil & Gas, Water, etc.) that support our daily lives and in the manufacturing industry. Since ICS has a dedicated network and is constructed with using ICS manufacture original hardware, software and protocol for each plant, it was deemed to be relatively stronger against cyber attacks. On the other hand, recently, Commercial Off The Shelf (COTS) devices are employed for ICS networks and interfaces with Enterprise, also IoT (Internet of Things) and AI (Artificial Intelligence) technologies are introduced for plant operation and maintenance. As a result, threat of cyber attacks that cause failures and malfunctions to important infrastructure are increasing, and countermeasures against the cyber attacks will become more and more important. In this paper, the threats of cyber attacks for ICS are reviewed and the countermeasures that can be taken in FEED (Front End Engineering Design), EPC (Engineering, Procurement, Construction) and O&M (Operation & Maintenance) are discussed.

****

1. はじめに

プラントの制御システム ICS(Industrial Control System : 産業用制御システム)[脚注i]は，我々の生活に身近なものから，生活を支える重要インフラ(電力，ガス，水道等)や製造業などで幅広く利用されている。従来の ICS は隔離された企業独自のネットワークを持ち，プラントごとにハードウェア,ソフトウェアおよびプロトコルなどが個別に構築されており,サイバー攻撃に強いとされてきた。しかしながら、昨今の ICS では、情報が一般公開された汎用デバイスの採用が進み、また、外部との

オープンネットワークを通して IoT(Internet of Things)や AI(Artificial Intelligence)等が活用されるようになった。その結果，ICS では常にサイバー攻撃の脅威に曝されており，重要インフラで故障や不具合が発生するリスクは増加の一途を辿っている。

本稿では ICS のサイバー攻撃に関する脅威について考察し，プラント建設における FEED(Front End Engineering Design)，EPC(Engineering, Procurement, Construction)および O&M(Operation & Maintenance)の各フェーズで，今後コントラクターが検討すべき課題について考察する。

2. デジタル化とサイバー攻撃

2.1 デジタル化の動向

デジタル技術を活用した業務効率化や高度化の動きが世界的に加速している [1)]。重要インフラの機器等のデータを仮想空間から収集し，メンテナンスの時期などを効率的かつ効果的に検知できるようになった一方，サイバーテロの発生件数は増加している。特に COVID-19 の発生後，テレワークが増えたことなどが起因し，リモートデスクトップ経由での通信を狙い撃ちにしてメールや SNS 等を用いた標準型攻撃，フィッシングサイト，マルウェア，ランサムウェア[脚注ii]や DDoS [脚注iii]，テレワーク環境を狙った情報流出などのサイバー攻撃が発生している [2)]。

重要インフラの保守・保全分野では，VR(Virtual Reality)や AR (Augmented Reality)などを用いてメンテナンス手順を見える化し,熟練工の不足を補う取り組みが始まっている。一方,EPC フェーズでは, プラント内の制御をコントロールルームで監視し, 手動又は有線ケーブルで信号を送ることで操作を行う従来の方法から, ワイヤレス計装を用いた運転監視方法も注目されてきている。これは計装ケーブル及び資材の低減, それによる配置設計の簡素化および工数の低減, そして工期短縮などを期待するものであり, 顧客(プラントオーナー)から請負会社(コントラクター)に対して提出される引き合い書類(Invitation to Bidder：ITB)に要求が入ることもある。

昨今，Society 5.0 が内閣府から提唱され，物理空間(Physical Space)から仮想空間(Virtual Space)へと業務を移行する組織が増加している。しかしながら，デジタル化による経済性・利便性の向上は一側面から見た評価であり，上述したようなサイバー攻撃が起こりやすくなっている側面もある。デジタル化による経済性や利便性の向上をデジタル化の進度として捉え，サイバー攻撃の頻度との関係性を見ると、両者は図 1 に示す比例関係にある。サイバー攻撃の発生は，組織の重要な情報の漏洩から不正使用により，顧客，取引先などステークホルダーを始めとする社会経済からの信用の失墜及び設備復旧までの機会損失など事業継続を脅かすインシデントとなりえる。このため、高い安全性が求められる重要インフラを手掛けるコントラクターには、物理空間と仮想空間を融合することで生産効率を高めると同時に FEED や EPC 段階でサイバー攻撃の発生リスクへの対応が求められている。

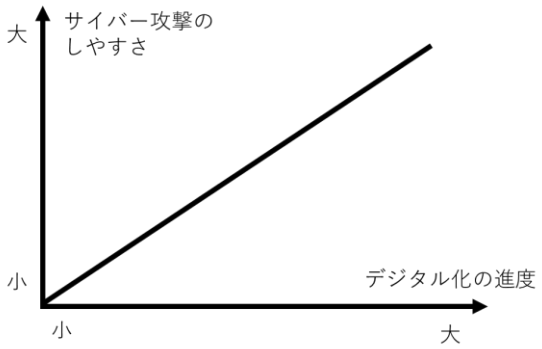

図 1　デジタル化の進度とサイバー攻撃の発生頻度

2.2　サイバー攻撃の動向

国立研究開発情報通信研究機構(NICT)は，大規模サイバー攻撃監視網（NICTER）のダークネットを活用し，グローバルにサイバー攻撃が起きている状況を観察している [3)]。この報告書によると， 2009 年から 2018 年の間でサイバー攻撃は約 60 倍になっているとしており，2017 年から 2018 年までの推移は 1.4 倍になっていることから，年々サイバー攻撃のリスクは増加傾向にある。中でも IoT 機器に対するサイバー攻撃は，特定の脆弱性を狙った攻撃が増加傾向にあるとしており，重要インフラに IoT 機器を設置することで利便性が上昇する一方で，IoT 機器や機器ベンダーからの納品物にマルウェアが仕込まれることや脆弱性が見つかること,バックドアが仕掛けられる可能性などのサイバー攻撃のリスクも検討せざるを得ない。また COVID-19 の発生を起点としたリモートワークの浸透などによってもランサムウェア等のサイバー攻撃を受ける事例が確認されており，既存の事業活動では発生頻度が低かったサイバー攻撃が表出化し易い時代になっている。。図 2 は IPA(独立行政法人情報処理推進機構)が公開している「制御システム関連のサイバーインシデント」事例を基に作成したものである [4)]。これは制御システムへのサイバー攻撃が行なわれた事例を示している。サイバー攻撃関連の調査結果や対策指針などが国立研究開発情報通信研究機構など各機関から多数報告され、昨今では重要インフラへのサイバー攻撃の事例を比較的容易に調査が出来る環境が整ってきている。

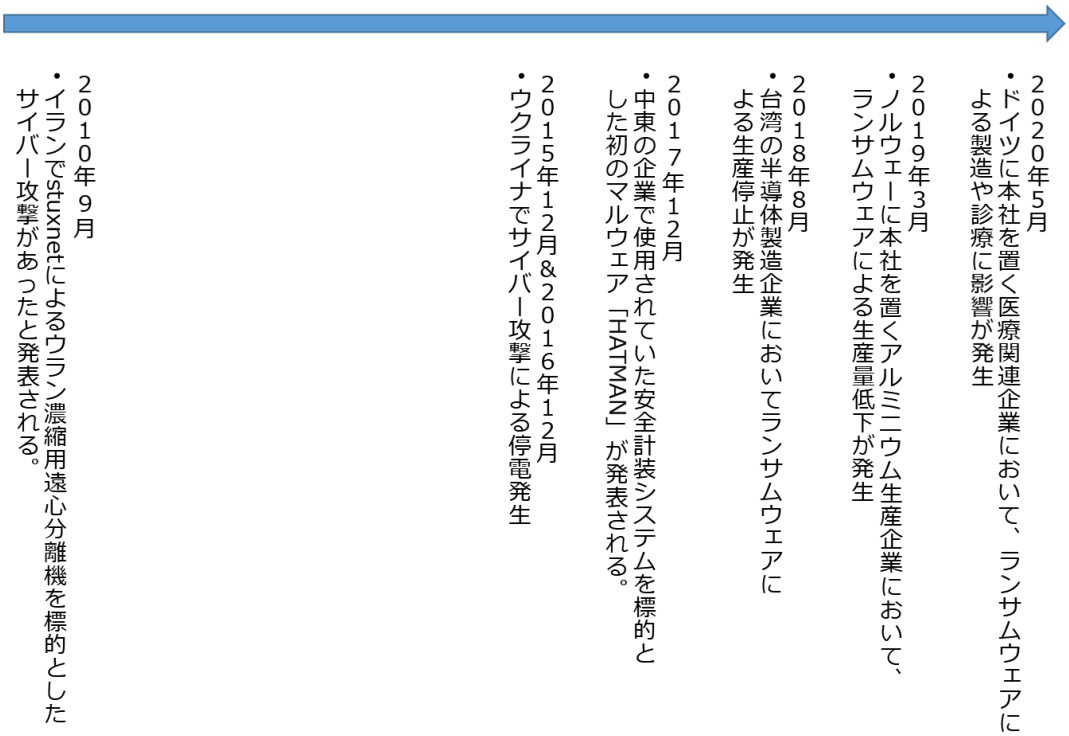

図 2　制御システムで発生したサイバー攻撃事例 [4)]

2.3　情報システムと制御システムのセキュリティの考え方

2.3.1　セキュリティに対する考え方

従来のサイバー攻撃では，家庭や企業などで利用されるパーソナルコンピューター(PC)を経由して個人情報等が流出する事例が多かった。このため，JIS Q 27002(ISO/IEC 27002)では情報システム(Information Technology：IT)のセキュリティとは，「情報の機密性(Confidentiality：C)・完全性(Integrity：I)・可用性(Availability: A)を維持すること」であるとしている [5)]。ここでは、アクセスを許可された者のみがアクセスできる状態を確保することを機密性，これと情報の改ざん・破損等をされていない状態を維持することを完全性，そして情報へのアクセスを認めた者のみが中断されることなく情報資産にアクセスする状態を可用性と呼んでいる。これは CIA と呼ばれ，IT セキュリティを担保するための重要な要素とされている。IPA[6)]の報告では，情報システムは CIA の順で重要度が高いとされている一方，重要インフラの制御技術(Operational Technology：OT)では完全性を担保することが難しいとの意見 もあり，重要度は可用性が最も重要で，その次に完全性，そして機密性になるとしている。

表 1　OT と IT の情報セキュリティの考え方の違い [6)]

	OT	IT
セキュリティ優先順位	A.I.C (可用性重視)	C.I.A (機密性重視)

セキュリティ対象	設備，製品，サービス	情報
稼働年数	10-20 年	3-5 年
稼働時間	24 時間 365 日	通常業務時間内
運用管理	現場技術部門	情報システム部門

C:情報の機密性 I: 情報の完全性 A: 情報の可用性

2.3.2 OT のサイバー攻撃への対応状況と課題

IPA の実態調査報告書 [6)]を見ると,「自社の保有するすべての制御システムの脆弱性対策に取組んでいる」と回答した企業は 21%に留まり,「制御システムの脆弱性対策に取組んでいない」と回答した企業は 43%である。重要インフラ企業でも 27%は脆弱性対策に取組んでいない。脆弱性対策を進める上での主要な課題としては，以下の通りである。

(1) 対策へのコスト
(2) 社内外の体制・人員の不整備
(3) 脆弱性対策の実施が困難な事業環境

従来 IT はオープンネットワークであり，OT はクローズドネットワークとされてきた。昨今の技術変化によって OT 側はクローズドネットワークとしながらも，多くの IoT 機器がオープンネットワークに繋がるようになっている。OT は 24 時間 365 日の安定稼動が必要とされることから，重要インフラに据えつけられた機器は高い頻度で付け替えられず，常時ウイルス感染や不正アクセスなどのサイバー攻撃のリスクにさらされることになる。また，昨今の OT では、システムの統合化や広域化により,サイバー攻撃による感染が広がり易く,さらに汎用アーキテクチャの採用が進んだため,感染の容易性も増大している。このような背景もあり，当社が顧客から受領する昨今の ITB の中には「OT に関するサイバーセキュリティ対策」についての要求が入ることがあり，サイバー攻撃の発生確率が増える状況の中での時代の要請となってきている。

上述に加えて，昨今，当社ではワイヤレス計装の導入要求を受けることが増えてきている。ワイヤレス計装が導入されている重要インフラは現状少ないため，筆者らが調査する限りサイバー攻撃の事例は確認できないが，今後ワイヤレス計装の導入が進めば，アクセスの自由度が高くなるので感染・影響拡大のリスクが生じる。そういった事例が出る前に顧客とリスクを共有し，さらに設計段階から対策を検討できるのは制御システム構成及びシーケンスを検討しているコントラクターだけと考える。したがって，本稿では，コントラクターが EPC にて OT セキュリティを検討するための課題を FEED や EPC の業務性質から考察する。

3．　重要インフラと OT セキュリティ

3.1　IT と OT のセキュリティ思想

本節では，2.3.1 にて IPA[6]が報告している IT と OT のセキュリティの違いについて考察する。IPA の報告書 [7]によれば、OT セキュリティのオープン化[脚注iv]に伴うセキュリティリスク対策は,「情報システムとの連携」に加え,「汎用製品」,「標準プロトコル」への対策の観点が必要とされており，もともとオープン化が前提となっている IT システムとは情報セキュリティに対する考え方が異なっている。

IT セキュリティでは脆弱性対処方法が確立される前の攻撃などに対応するため，システムのインストール，アップデートを PC の未使用時間帯に行い，その後再起動によってシステムに反映する。一方の重要インフラであるプラントのライフサイクルは，およそ 20 年から 30 年である。この期間中にシステムのインストールやアップデートが可能なタイミングは、定期補修などで装置が停止する限られた期間のみである。この理由は, 重要インフラは一度停止すると再稼働に膨大なコストが掛かり，また稼働が安定するまでに時間を要する上，その間に重大な機会損失が発生するためである。また，IT セキュリティを向上させて PC を再起動すると，セキュリティをアップデートしたことで他のシステムに障害が生じることもある。これが OT セキュリティで発生してしまうと，重要インフラの重大事故に繋がる可能性がある。このような理由から，IT セキュリティは完全性を重視するのに対し，OT セキュリティでは可用性を重視している。重要インフラの場合，事業当事者の経済的な損失だけでなく, 周辺環境のことを考えて安全性を担保する責任もある。重要インフラが人の健康や環境などに影響を与えるものを生産し, あるいは生活に密接している場合には, 発生する事故は周辺環境への影響に加え，病院などの機器が動かなくなるなどの深刻な二次的被害に発展する可能性がある。また，重要インフラは周辺地域からの理解によって初めて事業活動が成り立っている。したがって，サイバー攻撃への対応を考える場合，IT 側の主張，OT 側の主張，そして安全性の側面から考えることになるが，重要インフラは周辺環境からの理解によって初めて事業活動が成り立つため，安全性が最優先でなければならない。

サイバー攻撃は USB メモリーやリモートメンテナンス回線からのウイルス感染, 端末の入れ替えや内部犯行など感染経路は多種多様であり，日々進化している。このことからも，サイバー攻撃の対策を完全に行うことは現実的に考えて実現不可能である。事実，IT セキュリティをどれだけ強固にしてもセキュリティソフトウェアがウイルスを検知・除去できるのは，一般的に認知ができているものに限定され，新規のウイルスに対しては機能しない。

IT と OT のサイバー攻撃は悪意ある攻撃であることには変わりはないが，IT は機密情報の漏洩や身代金が目的となりやすい一方，OT は重要インフラの運転を停止させることで重要インフラ自体に損害を与えることが目的となることが多い。

3.2　OT セキュリティとコントラクター

顧客とコントラクターの双方あるいはいずれかの担当者が IT 系の出身である場合，OT 側の特性を考慮しない対策が取られる懸念がある。また，昨今 EPC の工期が短縮されている実情を踏まえると，制御関連の設計要件を確定し，図面を早期に確定させ，引き合いや発注への影響を抑えることは現実的に難しい。コントラクターから曖昧な要求でベンダーに発注することで発注品のサプライチェーンでのセキュリティの確保が難しくなり，後々，ベンダーから顧客あるいはコントラクターに対して追加要求を受けるリスクに繋がる。さらに，サイバーセキュリティでコントラクターが担保する条件について顧客と合意しておかなければ，重要インフラの引き渡し後にサイバーテロが起こった場合，責任所在が不明瞭になり，責任の所在について顧客やコントラクターとの間で論争が生じるリスクも存在する。

日々脆弱性が見つかり，あらゆる手段でのサイバー攻撃が増える昨今の状況では，完全防御は実現不可能な要求である。まずは，年々サイバーセキュリティに関する規格が変化する現段階においてどの規格に適合させるのか，そして規格が変更された場合にどのように対策を取るべきかについて考えて，顧客との契約に定めておくことが現実な対応となる。これに対して，顧客又はコントラクターの OT セキュリティ担当者がセキュリティの思想である「完全性の担保」を重要視するあまり，設計思想の違いから意見がまとまらないことで各種設計への反映が遅延するリスクも考えられる。これは結果として機器の調達遅延，建設工事への影響を及ぼすことに繋がる。

3.3　**重要インフラの建設ワークフローと** OT **セキュリティ**

ITB で顧客からサイバーセキュリティ対策について要求される場合，顧客にもコントラクターにも OT のサイバーセキュリティについての基準がない場合がある。このような場合，JIS Q 27002 (ISO/IEC 27002)[5)]などの基準が参考にされるが，OT のサイバーセキュリティの対策をどのように捉えるべきかが示されているに留まり，どのように対策を採るべきかの”How to”までは述べられていない。サイバーセキュリティ対策の要求が顧客から出された場合，”How to”を FEED/EPC/O&M のどこで検討するのかは，顧客とコントラクターにとって重要な課題である。

図３のワークフローの中で重要インフラが稼働するまでは，OT セキュリティのリスクは顕在化することは考えられないため，FEED や EPC の段階での情報漏洩は IT セキュリティの問題となる。しかし，試運転を経て重要インフラが稼働開始すると，OT セキュリティのリスクはインフラの稼働時間の経過と共に高まってゆく。図３は重要インフラ建設の一般的なワークフローである。設計の基本的な思想は FEED で固まってしまうことが多く，重要インフラが稼働した後の安全思想の大枠は，EPC の見積もりの段階で決まる。従って，EPC の見積もりの段階では重要インフラが稼働した後の設計や安全思想の大枠は決まってしまう。また，EPC が短納期の場合には，契約前の段階で Early Work と呼ばれる作業を行い，納期に間に合うようにすることもある。このようなプロジェクトでは，EPC の最中に OT セキュリティの対応思想を検討していたのでは制御システム構成及びシーケンス等の確定が遅くなり，結果として建設工事に影響が出る可能性が高い。納期の長短にかかわらず、い

ずれの EPC 案件においても、OT セキュリティの規格対応をどうするか等については、顧客とコントラクターが一体になって協議・対策を進める必要がある。

前述に加え，EPC の上流設計では，P&ID(Piping & Instrument Diagram)に基づいて HAZOP(Hazard and Operability Study)や SIL（Safety Integrity Level）Study 等の安全性評価が行われる。この結果として安全上の問題が見つかった場合には、オペレーション上の問題を網羅的に洗い出し，設計に反映させる。しかしながら，昨今は安全計装システム(Safety Instrumented

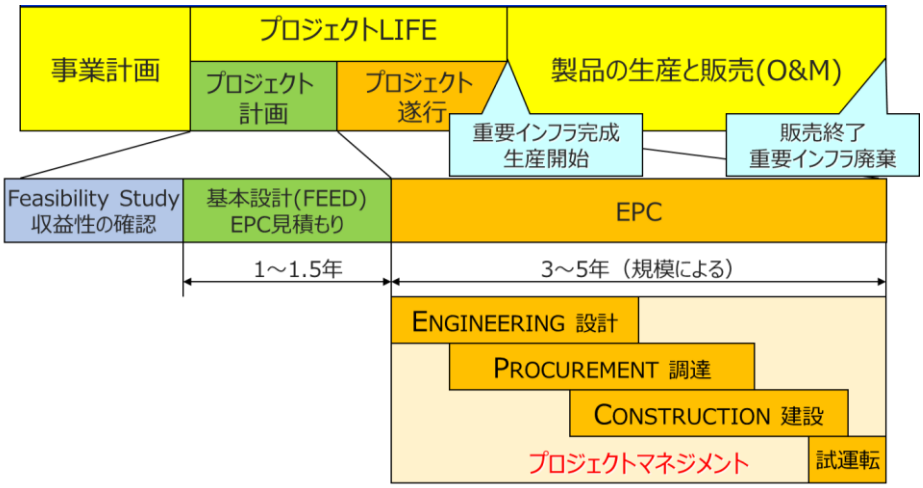

図 3　一般的な重要インフラのプロダクトライフサイクル

System：SIS)のコントローラー自体の不正操作の事例 [8)]もあり，プログラムを書き換えることで安全装置の本来の機能を不能にし，機器が物理的に破壊される事例が確認されている。このため，サイバー攻撃の対策検討では，本来の安全設計に加えて，SIS のプログラムが書き換えられた場合の対策についても検討が必要になっているのが実情であり，EPC での対応を考慮する段階に来ている。

3.4　重要インフラの建設への影響

現行では重要インフラの OT セキュリティ対応は、O&M 段階で行われることが多い。この対応を新しく建設する重要インフラに対して行う場合，安全設計などの思想の大部分は FEED 又は EPC の設計段階で定まってしまう。その後の段階で，EPC の要求事項に OT セキュリティが追加で盛り込まれるようなことがあると，安全設計の検討完了後に制御システム構成及びシーケンスの見直しなどの作業が追加になり，制御機器等の調達開始時期が遅延するなど、後続作業に大きな影響を及ぼすリスクがある。これは重要インフラの工期，つまりは製品の生産と販売に影響を与えかねないリスクであり，この取り扱いについても顧客とコントラクターの間での慎重な協議が必要である。

OT セキュリティの対策は，制御機器のベンダーを中心に機器の技術開発が行われ，顧客側では O&M 段階の重要インフラに対する対策を取り始めている。しかしながら，コントラクター側では顧客要求がない限り，対応をしないなど，組織的な対応の整備が遅れていることが多い。OT セキュリティ対応が組織的に整備されないと、セキュリティの要件確定がネックとなり，EPC や O&M の段階

において設計の長期化による建設の遅れや、設計不良による O&M での追加工事などの問題を生じさせる可能性が残る。今後，このようなリスクを回避するべく，コントラクターには FEED，EPC および O&M の各段階において，OT セキュリティに関するリスク分析と対応指針の策定を，顧客と共に積極的に進めていくことが求められる。

3.5　EPC への影響

EPC の段階で OT のサイバーセキュリティ要求が顧客とコントラクターの間で固まっていない状態が長引けば，コントラクターがベンダーに対して提出する技術要求への盛り込みが遅くなる。結果としてベンダーへの要求事項が確定せず，引き合いの遅延や長期化を引き起こす可能性が高く，納期や調達コストに少なからず影響を与える。顧客要求として EPC の ITB に入れる場合，顧客側の求める OT のセキュリティとコントラクターとして取れる対策のすり合わせを FEED の段階で実施し，OT セキュリティを含めた安全設計が完了していることが望ましい。また，FEED で検討しきれない場合は，HAZOP/SIL あるいは，制御系に注目した Control Hazop としての安全検討が完了した段階から同時並行で OT セキュリティの対策プロジェクトを立ち上げ，EPC とは別に検討を進める方法も考えられる。リスクに対しては保険を適用するような考えもある。

サイバーセキュリティの保険について調査をしてみると，IT や OT に対するサイバー攻撃の頻度が増加し，世間の関心が高まるにつれて，最近ではサイバー攻撃に対する保険の販売が始まっている。ただし、この保険で対象とされるのは，損害賠償や対応費用，サイバー攻撃の調査費用などであり，第三者に影響が証明できる範囲に留まっている。保険を適用する場合，自動車保険などと同様，保険業者に対してサイバー攻撃が起こった証明義務が生じる。この際に行われるデータ収集と解析，分析，報告の流れはフォレンジックと呼ばれる。保険対象の重要インフラにサイバー攻撃が行われた場合にもフォレンジックを行う。重要インフラでは休止期間中に発生する機会損失の低減を図るため、サイバー攻撃の検知からフォレンジックを実施して再稼働させるまでの RTO(Recovery Time Objective) をいかに短縮できるかが，事業継続の上でも重要になる。

重要インフラはインフラの規模や制御の思想，時代毎の規格の移り変わりに左右され，二つとして同じものは存在しない。類似の重要インフラが存在したとしても制御系の機器の調達先の違いなどを含め，多少の変化は生まれる。このため，同じ思想で RTO の短縮方法を検討するにしても，効果があるとは限らない。このような観点から，ICS のサイバーセキュリティの考え方には，いかに事業を継続させるかに焦点を当てた Business Continuity Management (BCM：事業継続マネジメント) [脚注iv]の考え方が重要とされ，サイバー攻撃が起きた際にいち早く状況を察知し，安全に重要インフラを停止，又は部分的に切り離しを行える設計にしておくことも対応として考えられ，その場合には，Business Continuity Plan(BCP：事業継続計画) [脚注v]が必要である。この事業継続をするための重要インフラの設計ができるのは長年，重要インフラの EPC を担当してきたコントラクターだけであり，今後益々その役割は重要となってくる。コントラクターには，以下の OT セキュリティへの対

策が求められる。

(1)　OT にサイバー攻撃を受けた際の事業継続までを考慮した安全設計の基本思想の策定
(2)　顧客が過去又は新規建設する重要インフラのサイバー攻撃を受けた場合のリスク評価指標の策定
(3)　安全設計思想を検討するタイミング
(4)　サイバー攻撃対応をする場合のベンダー選定や要求事項の策定
(5)　上記，(1)-(3)を EPC にて実施する場合のリスクシナリオの策定
(6)　OT セキュリティのコントラクターとして補償できる範囲の決定

4. おわりに

プラントのデジタル化に対する顧客要求と，これに伴いリスクの増加が予想されるサイバー攻撃への対策は，今後ますます重要になることが予想される。現状確認できるだけでも，重要インフラに対して年間数件から数十件のサイバー攻撃が発生しており，その頻度は増加傾向にある。この一方で，顧客とコントラクターの間で，O&M で OT がサイバー攻撃を受けた場合を考慮した設計を検討している事例は確認されていない。

弊社が顧客から受領した ITB では，数件のプロジェクトで FEED や EPC で OT セキュリティの対策検討の要求が出ており，今後，同様の要求が出されるケースは益々増えてゆくものと予想される。この問題はベンダー中心として対策が行なわれていた状況から，顧客やコントラクターでも影響と対策を無視できない状況になりつつあるのが現実である。

本稿では，OT セキュリティに関する基本事項をまとめ，サイバーセキュリティ関連の文献であまり議論されない EPC への影響についてコントラクターの視点から考察を行い，今後コントラクターが検討すべき 6 つの課題を提示した。今後，社内外を通して 6 つの課題について解決を図っていければ幸いである。

脚注i　産業用制御システムは ICS(Industrial Control Systems)と呼ばれ、その制御技術は OT(Operation Technology)と呼ばれる。

脚注ii 「Ransom(身代金)」と「Software(ソフトウェア)」を組み合わせた名称であり，マルウェアの一つ。端末内のデータを暗号化して使えない状態にしたりして，解除のために身代金を要求するウイルス。

脚注iii　Distributed Denial of Service の略。インターネット上の複数の機器から特定のネットワーク／コンピュータに一斉に通信を行い，過剰な負荷をかけるサイバー攻撃のこと。

脚注[iv]　事業継続計画とは，企業の事業継続に影響を及ぼすリスクが顕在化した場合に，企業が早

期にサービスを提供するための事業復旧の方針や体制，手順等を示した計画書のこと。

脚注[v]　重要インフラでは，AIC の順番での対策が重要であるが，CIA の順番で情報セキュリティの対策を考えてしまう等の問題が生じる。

引用文献

1) 藤井渉，濱田佑希，ペトロテック，42, (7), 500 (2019).
2) NIST サイバーセキュリティ戦略・サイバーセキュリティ 2020 の概要(20207/27)
3) NICTER 観測レポート 2018，
https://www.nict.go.jp/press/2019/02/06-1.html (2019/2/6)
4) 独立行政法人情報処理推進機構,制御システムのセキュリティリスク分析ガイド補足資料:「制御システム関連のサイバーインシデント事例」シリーズ
https://www.ipa.go.jp/security/controlsystem/incident.html (2020/9/8 更新版)
5) 中尾康二，”ISO/IEC27002(JIS Q 27002) 情報セキュリティ管理策の実践のための規範”，日本規格協会 (2013).
6) 独立行政法人情報処理推進機構セキュリティセンター，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 (2009).
7) 独立行政法人情報処理推進機構，制御システムユーザ企業の実態調査報告書，(2016) .
8) CYBER X, https://cyberx-labs.com/ja/oil-gas/ (2018/2/14)