制御系 SIRT の機能を備えるための手引き

制御システムを対象としたインシデント対応に備えて考慮すべきポイント

（CSIRT マテリアル補完資料）

製造業分野

Ver.1.0

一般社団法人 JPCERT コーディネーションセンター

2024 年 3 月 27 日

目次

1. はじめに

一般社団法人 JPCERT コーディネーションセンター（以下、「JPCERT/CC」という。）では、産業界における制御システム（Industrial Control System 以下、「ICS」という。）のユーザー組織に対して、ICS セキュリティに関する種々の情報発信のほか、ICS に対するセキュリティアセスメントや自社で活用する ICS セキュリティポリシーの策定支援等、これまでにさまざまな ICS におけるセキュリティ対策の支援を行ってきた。こうした JPCERT/CC の取り組みも含め、さまざまな組織の取り組みもあり、種々の産業界で ICS のセキュリティが向上しつつあるものと考えている。その一方、特に製造業において、国内事業者でもサイバー攻撃による被害が発生し、中には公表される事例が散見されるようになってきた。
こうした中、JPCERT/CC が開催する「制御システムセキュリティカンファレンス」でのアンケートや業界団体および個社からの相談、有識者との意見交換等を通じて、製造業の ICS セキュリティ担当者の関心が、ICS を対象としたセキュリティインシデントの対応体制の整備等、より有事を想定した備えに進みつつある状況が見えてきている。また、経済産業省のサイバーセキュリティ経営ガイドラインの付録「サイバーセキュリティ体制構築・人材確保の手引き [1]」においても、ICS を対象としたセキュリティインシデントの対応体制に関する記載がなされている。

2. 本書について

2.1. 本書の作成背景

上述した ICS を対象としたセキュリティインシデントの対応体制への取り組みが進みつつあるものの、セキュリティインシデント対応体制（Security Incident Response Team 以下、「SIRT」という。）の構築や運用に関連した文献の中で、「ICS を対象とする際に考慮すべきポイントや要件」が記されたものは、JPCERT/CC が確認した限り、ほとんど見られなかった（本書の初稿執筆時点）。文献が一部存在する [2] が、作成年が古く、その内容は本書の初稿執筆時点の ICS を取り巻くセキュリティ事情が必ずしも反映されていない点、特定国の国内事情に沿った内容となっている点等が見られた。そのため、日本の製造業における ICS セキュリティ担当者が、ICS を対象とした SIRT（以下、便宜的に「制御系 SIRT[3]」という。）に必要な能力等を検討する際の手がかりが少なく暗中模索となっており、JPCERT/CC へ同 SIRT の構築初期段階と思われる組織の ICS セキュリティ担当者からご相談をいただくケースが少なからずある。「制御系 SIRT」が備えるべき能力およびそのために必要なその他の考慮すべき事項等に関する要件が求められていた。

---

[1] サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き第 2 版
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

[2] 推奨プラクティス：工業用制御システムにおけるサイバーセキュリティインシデント対応能力の開発
https://www.jpcert.or.jp/research/2010/CSincident_response_20100330.pdf

[3] 「制御系 SIRT」は、「FSIRT」「OT-SIRT」等と呼称されることもある

2.2. 本書の目的

上述の「制御系 SIRT」を適切に構築、運用していくためには、備えるべき能力とそのために必要な要件の検討と整理が必要であった。求められる能力と要件はさまざまあるが、JPCERT/CC がこれまでに対応してきた問い合わせ等の中で良くみられた課題のうち、構築を検討する担当者が構築初期に直面する可能性がある課題とその解決に資する要件の整理について、JPCERT/CC と複数の製造事業者における ICS セキュリティ担当者で形成したコミュニティー（以下、便宜的に「ICS セキュリティ担当者コミュニティー」という。）で検討を行ってきた。同コミュニティーの参加者は、化学、機器製造等の複数の製造業種で、かつ 20 社以上の ICS セキュリティに積極的に取り組む製造事業者であり、延べ 35 名以上の ICS に関わるセキュリティ担当者と上述の要件検討に取り組んできた（本書初版執筆時点）。本書は、その取り組みの中から、製造業において、「制御系 SIRT」が備えるべき能力やそのために必要な要件等について、実務者ベースで検討し、これまでに分かってきた知見をまとめたものである。そのため、本書は必ずしも必要な項目を現段階で網羅的に記載したものではなく、今後も取り組みの結果をフィードバックし、必要に応じて文書の改訂を行っていくことを想定している。
よって、本書の記載内容は参考情報であり、業種や個社の諸事情によっては、必ずしも適切な解を提示するものとならない場合もあるが、ICS に関わるセキュリティ担当者が「制御系 SIRT」の新規構築の要件を検討する際の参考として活用し、適切な構築につながる一助としていただくことを目的としている。また、すでに「制御系 SIRT」を構築している ICS セキュリティ担当者は、自組織の「制御系 SIRT」の能力や活動と照らし合わせ、改善策を検討するための参考資料として活用していただくことも想定している。

2.3. 本書の内容のスコープ

ICS を対象とするインシデント対応においては、CSIRT 機能で対応できる点もあるが、同機能は情報システムにおけるセキュリティインシデントの対応をベースとしており、上述したように、ICS 特有の事情が考慮された記述が見られない。本書では、次の図 1 が示すように、「ICS ならではの考慮点」（オレンジ色）を主なスコープとする。

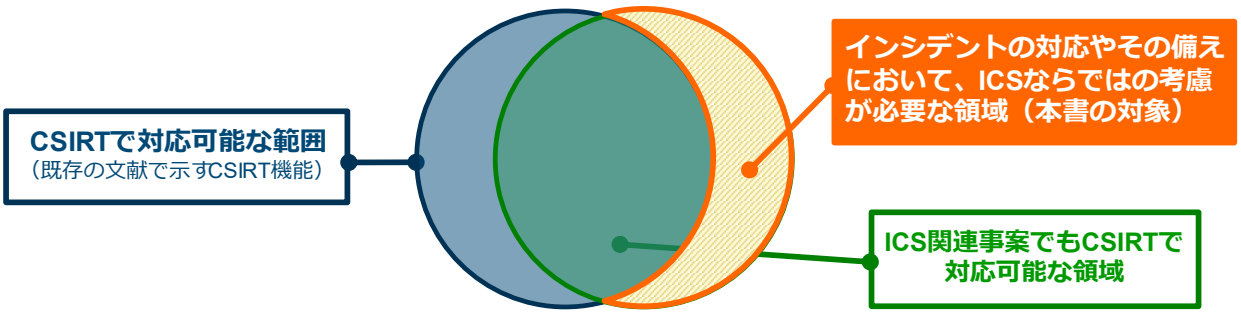

図 1　CSIRT の対応範囲と本書の対象の関係（イメージ）

このため、本書が想定する次の読者（a および b）が CSIRT 機能を理解していることを前提条件として、本スコープに関して述べる。CSIRT に求められる主な機能については「CSIRT マテリアル [4]」を参照いただきたい。

なお、本書の内容は、上述の製造事業者とのコミュニティーで取り組んで得た知見をもとにしており、本書執筆時点で整理できた要件に限っているため、制御系 SIRT の構築に必要な要件をすべて網羅しているものではない。

想定読者：

a) 主に、CSIRT 機能を理解した上で、製造業における「制御系 SIRT」または準ずる体制の構築を検討する担当者、同 SIRT 機能の改善を検討する組織の担当者
b) 上記の検討等を支援するその他の ICS セキュリティに関わるステークホルダー（ICS 関連の製品/サービス提供者、ICS セキュリティサービス提供者等）

本書を活用する際の留意点：
CSIRT の形態においては、専任の要員で構成されるいわゆる「消防署型 CSIRT」や兼任の要員で構成されるいわゆる「消防団型 CSIRT」のいずれか、またはそれらの混成型等があり、実態としては各組織事情に応じて組織されているため、これらの形態に留まらないものと思われる。本書で述べる「制御系 SIRT」の機能においても、CSIRT 内にその能力を備える形態もあれば、CSIRT とは別に組織する形態も見られる。前者の場合も後者の場合も、多くは兼任の要員で構成される例が見られ、CSIRT と別に組織する場合でも、CSIRT と連携するケースが多いと思われるが、その連携形態も一様ではない。どのような組織形態にするのかは、各組織事情に応じる必要があるため、本書ではいずれかの形態にすることを求めるものではない。

本書では、あくまで、これまでの CSIRT 関連文献ではみられない「ICS を対象とした SIRT が備えるべき能力およびそのために必要なその他の考慮すべき事項等に関する要件」を明らかにすることに重きを置き、読者各位の所属する組織の事情に応じて、読み替えつつ活用いただくものとして作成している。
なお、本書に記載の要件等について、JPCERT/CC の今後の取り組みの中で、新たに分かったことがあれば、適宜、追加や改訂を行う場合がある。

2.4. 本書が想定する ICS モデル

図 1 では、ICS 関連のインシデント対応やその備えにおいて、ICS 考慮が必要な領域があることを視覚的につかんでいただくために、イメージ図で示した。ここでは、巻末の参考文献欄に掲載した一部の文献および ICS ベンダー、ICS エンジニアリングのいくつかの組織から伺った情報を参考にしつつ JPCERT/CC にて作成した、今後より多く構築される可能性がある形態で、かつ典型的な製造業における ICS の Purdue モデルを示す。製造業の業種によっては、さまざまな ICS が存在するが、DX 推進等

[4] CSIRT マテリアル
https://www.jpcert.or.jp/csirt_material/

を理由として、ネットワーク接続やクラウドの活用がより進展することが見込まれている。本書では、こうした状況を踏まえて、次の ICS Purdue モデルを前提に論じる。

なお、ICS 関連のインシデント対応を考える上で、ICS におけるサイバーセキュリティ上のリスク要因や対策等の検討を行うには、DMZ から Level0 にかけての設備やその運用等により注目するが、「制御系 SIRT」の活動において留意すべきなのは、ICS 自体のセキュリティ上の保護に留まらない、ICS の操業や事業継続への影響を最小化することにあり、Level 4 以上のレイヤーも論点から排除するものではない。

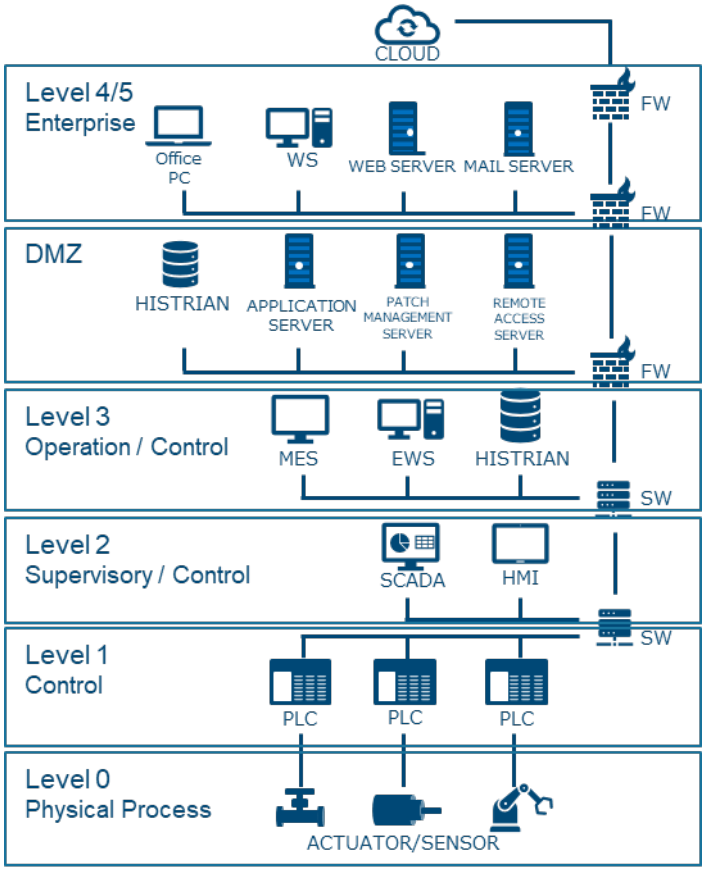

図 2　本書の ICS Purdue モデル（参考文献等をベースに JPCERT/CC が作成）

3. ICS を対象とする SIRT に求められる要件

SIRT が ICS を対象に適切に活動するには、ICS 特有の事情を考慮する必要があり、そのために構築時から認識しておくべき要件がある。このうち、これまでに明確になって来た要件を以下に記載する。
なお、「制御系 SIRT」の要件を「組織体制の構築時に求められる要件」と「インシデント対応の機能を備える際に求められる要件」に大別して述べる。

3.1. 組織体制の構築時に求められる要件

3.1.1. 組織活動の考え方：セキュリティとセーフティの相互理解と調整

一般に SIRT は保護対象に対するサイバーセキュリティの確保を中心的な活動に据えるが、その活動の軸となる考え方は基本的に情報システムにおけるセキュリティ対策の考え方を参考にすることが想定される。現に、JPCERT/CC にお問い合わせいただくケースでも、そのような例が多い。
しかし、ICS をその保護対象とする場合、ICS の取り扱う対象が物理的な現象を伴うものであるという特性があることを踏まえ、すでに ICS の運用において長年培われて来た「セーフティ」の確保（例：ICS の操作卓は緊急停止等の即時操作ができるようログイン用のパスワード設定をしない、製造中止等でセキュリティ上のサポート対象外となった ICS 製品でも安全に操業するために必要な場合は使用する等）をセキュリティ対策が棄損するようなことがあってはならない。つまり、ICS におけるセキュリティ対策の推進は「セーフティ」の確保を前提に進めるように行う必要がある。こうした視点は平時、有事に寄らず、ICS のサイバーセキュリティを推進する際に考慮すべき視点である。

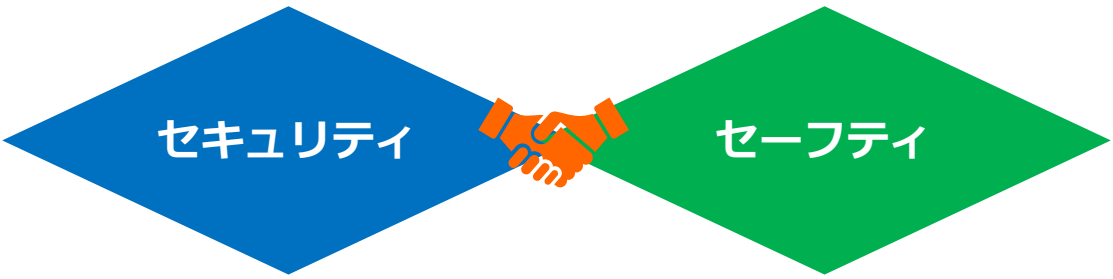

図 3 セキュリティとセーフティの相互理解

こうした視点を考慮するには、セキュリティの知見を有する担当者（情報システムセキュリティ担当者、CSIRT 等）とセーフティの知見を有する担当者（製造設備の保安担当者等）との相互理解と連携が重要であり、どちらかにのみ任せるのではなく、ICS において必要とされるセキュリティ対策を協力して検討し関係者間で調整して実装することが重要である。
実際、JPCERT/CC が把握している事例においても、このような関係者間での調整が行えている組織とそうでない組織では、ICS セキュリティ対策の進み具合が異なっている。前者では ICS セキュリティに関する対話が両者間でできているため、どちらか一方に過重な負担を強いるものではないことから、過不足の確認や役割分担も進み、ICS におけるインシデント発生時の対応への備えにもつながっているようである。一方、後者では ICS におけるセキュリティ対策も情報システム同様にセキュリティ担当者が行うべき、もしくは製造現場はセキュリティに疎いためセキュリティ担当者がいわば教える立場に立つ

べきといった考え方から協力関係が構築できず、一方への負担増等を引き起こし、ICS におけるインシデント発生時の対応への備えはおろか、ICS におけるセキュリティ対策状況の評価や必要に応じたセキュリティ製品の導入検討等、ICS セキュリティを進める上で行うべき基本的な対策が、製造現場関係者の協力を得られずに進まないといった ICS セキュリティ担当者からの声を聞くことがある。
組織内の関係構築が進まない理由はこれだけに留まらずさまざまな理由があるが、ICS セキュリティを推進するにはどちらか一方だけの取り組みでは進まない。両者は協力し合うパートナーであることを忘れてはならない。

3.1.2. 組織内関係者：ICS 関連のセキュリティインシデント対応に関わる関係者および部門等

本項では、ICS 関連のセキュリティインシデントが起きた場合に何らかの対応を行う可能性がある各関係者と想定される主な役割について記載する。
ICS 関連のセキュリティインシデントにおいては、事象およびその影響が情報システムのそれとは異なる場合があり、そのため、情報システムにおけるインシデント対応と同様の対応で進められる場合もあるが、事象によっては対応すべき関係者も異なることが想定される。
これまで、JPCERT/CC で確認している製造業における関係者とその主な役割を記載しておく。なお、あくまで参考であり、当該事業者の事情と発生事象の影響によってはこの限りではない点に留意いただき、ICS 関連のセキュリティインシデント対応の備えを行うにあたり、事前の関係者間連携の参考としていただきたい。

表 1 組織内の関係者および部門とその主な役割

ICS インシデント対応上の役割例	実担当者・部門例［職務］
全社的なセキュリティ上の確認・調整等	「CSIRT（専任/セキュリティ以外の職務との兼務含む）」［全社のセキュリティ担当］
ICS におけるセキュリティ上の確認・調整等	「制御系 SIRT（専任/CSIRT 兼務含む）」［ICS セキュリティ担当］
ネットワーク、端末におけるセキュリティ上の監視や対処等	「SOC（ICS 側の対応も含む）」［ICS 上のネットワークや端末におけるセキュリティ担当］
対処の工場側責任	工場責任者［工場管理責任］
生産計画・製造・製品供給の調整等	製品供給担当者［生産計画・製品供給責任］
製造設備の交換等	生産技術担当者、計装担当者［製造設備管理］
製造設備の安全確認・対処等	保安管理者［設備保安管理］
製造品の品質確認等	品質管理者［品質管理］
被害/影響を受けた製造設備の運用指示を受けた迅速な操作	製造オペレーター［製造設備運用］
製造設備に連携する IT 端末の対処	制御系の IT 管理者［制御系 IT 管理］
各種法規制の順守・違反における対応、法的対抗等	法務担当者［法的対応］
公表・取材等の広報	広報担当者［広報］
経営判断・措置	経営者［経営責任］

3.1.3. その他の要件

その他、組織体制を構築するには、その使命（役務等）、設置根拠文書（自組織向け ICS セキュリティポリシー等）、要員、予算等の検討と明記も必要である。

3.2. ICS に関するインシデントに対応するための機能を備える際に求められる要件

「制御系 SIRT」に求められる機能はさまざまあるが、中でも ICS に関連するインシデントへの対応は重要な機能である。本項では、インシデントにおける対応において、上述の「ICS セキュリティ担当者コミュニティー」で取り組んだ ICS に関連するインシデントマネジメントおよびインシデントハンドリングの機能において、JPCERT/CC で整理した要件を述べる。機能の構築や運用の参考としていただきたい。なお、CSIRT に関する多くの文献では、インシデントへの対応上の機能は、次のように整理されている

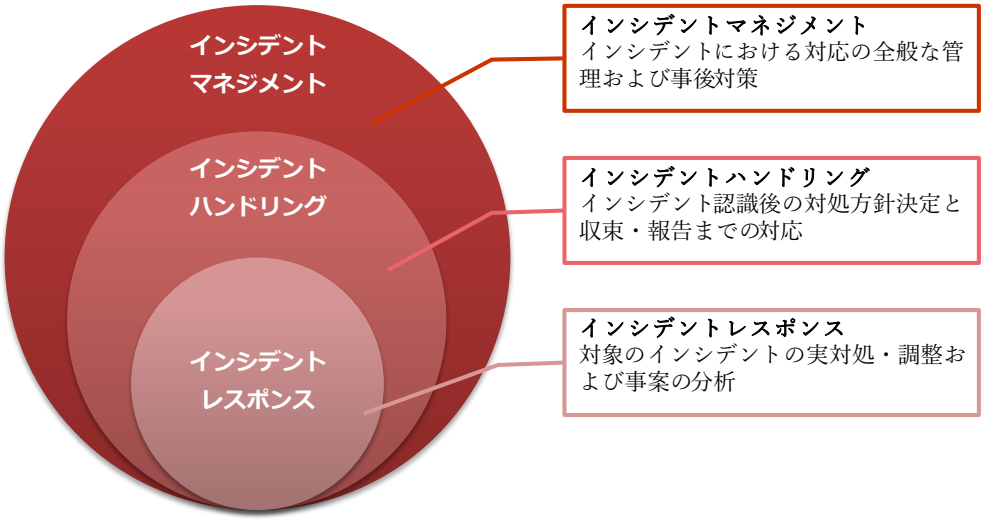

図 4 インシデントにおける対応の関係図

3.2.1. インシデントマネジメントにおいて求められる ICS を考慮した要件

SIRT のインシデントマネジメントにおける活動では、一般に次の項目等が取り上げられる。
CSIRT Service Framework および CSIRT マテリアルを参照した。

項目例）

- インシデントハンドリング
- 脆弱性の管理と対応
- 事象の把握と分析
- 意識の向上と知見の習得を目的とした啓発や教育

これらのうち、「脆弱性の管理と対応」は、インシデントの未然防止や、インシデント発生時の被害の低減のために重要であり、JPCERT/CC がこれまでに「制御系 SIRT」の担当者等との取り組みで注力してきた活動でもある。
「脆弱性の管理と対応」において、これまでに確認してきた ICS を考慮した場合のポイントについて、次に述べる。今後の「脆弱性の管理と対応」の参考としていただきたい。

a) 脆弱性の管理と対応

「脆弱性の管理」では、公表される脆弱性情報のうち、自組織で利用している ICS において、該当するものが無いかを把握できるよう、利用している ICS と脆弱性情報との関係を整理しておくことが重要である。そのためには、次の点を行うことが欠かせない。

- 利用している ICS 関連製品の棚卸し
- 棚卸し結果をもとにした資産管理表の作成
- 公開される ICS 関連の脆弱性情報の入手
- 資産管理表において入手した脆弱性情報の該当の有無を確認
- 該当があった場合の当該脆弱性の対応要否の検討

資産管理表は、入手した脆弱性情報と突き合わせができるように、少なくとも「ソフトウェア製品名（または機器名）」「バージョン」が必要であり、その他に「アップデートの適用有無」「アップデート日」等を記載しておく必要がある。このとき、組織内の対象製品を漏れなく把握するには、棚卸し関係者間でどういったものが対象となるのかのイメージを共有しておくことが重要である。セキュリティ対策と聞くと、外形的にパソコンのようなものだけをイメージする場合があり、ICS 関連製品の中には、そうしたイメージとは異なるものが種々あるため、ICS におけるセキュリティ観点での棚卸しの際は留意する必要がある。
また、利用している製品に組み込まれているコンポーネントまで把握して記載しておくと、脆弱性情報を入手した際、コンポーネントの脆弱性についても突き合わせができるため、より詳細に利用している ICS の脆弱性を把握することができる。なお、同資産管理表を最新化しておくために、定期的な棚卸しを行い、資産管理表に反映しておくことも重要である。
※ここで述べる「資産」は、脆弱性対応等の ICS セキュリティ対策の対象となる ICS 関連製品（例：ICS 付帯 PC や EWS およびそのソフトウェア、ICS/OT 向けネットワーク製品、ICS で使用する IoT 製品等）を指し、「資産管理表」はセキュリティ視点での管理項目を記載した表を指す

当該脆弱性の対応要否を検討する際は、対象製品の ICS における利用箇所や運用状況等を加味して、脆弱性を解消しない場合の ICS および事業における影響を評価し、対応すべきかを検討する必要がある。

図 5　ICS 関連製品の脆弱性情報の確認イメージ

「脆弱性の対応」では、上記の突き合わせによって、入手した脆弱性情報のうち、要対応となったものについて、次の「脆弱性に関する 3 つの対応方針」を検討して、いずれかを行う必要がある。

■　脆弱性に関する 3 つの対応方針
- アップデートやパッチの適用等による当該脆弱性の解消（根本的な対処）
- ワークアラウンドの実施による当該脆弱性におけるリスクの低減（低減対処）
- いずれの対処も行わず当該脆弱性の把握に留める（リスクの受容）

上記 3 つの対応方針を検討する際、可能であれば、根本対処を行って、脆弱性を解消することが望ましいが、ICS の運用状況や事業影響等の事情を踏まえた評価を行って、ワークアラウンドの採用もしくは対処せずにリスクを受容することもあり得る。

業種や製造品等の事情により、脆弱性対応による ICS への影響が事業に多大な影響を及ぼす場合があるため、脆弱性対応においては、単に入手した脆弱性情報に記載の ICS における直接的な影響のみを評価して方針を決定するのではなく、当該脆弱性に関連するシステムへの影響や事業影響の観点も交えて対応要否や対応方針の検討を行う必要がある。また、仮に対処せずにリスクを受容することになったとしても、そうしたリスクを把握しておくことができる。リスクを把握することができれば、すぐに対処できないものであっても、将来的に当該箇所への監視を強化する等の措置を検討することもできる。
このような「脆弱性の管理と対応」の活動は、ICS におけるセキュリティリスクを把握することに寄与する。

なお、脆弱性対応を行うには、ICS 関連の製品およびサービス提供事業者、構築や保守等を行うエンジニアリング事業者等の ICS ユーザー組織以外のステークホルダーとの連携が不可欠である。脆弱性の解消は、それぞれの立場においても有益であることを相互に理解し、協力関係を築いておくことも忘れてはならない。

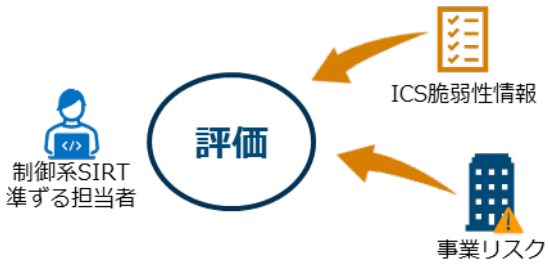

図 6　事業リスクの観点も交えた評価イメージ

3.2.2. インシデントハンドリングにおいて求められる ICS を考慮した要件

3.2.2.1. インシデント発生時の対応姿勢：事象に応じた役割（旗振り、調整等）を担う

一般に、情報システムにおけるセキュリティインシデントが発生すると、CSIRT が対応の主体になるが、前項までにしるした事象を含め、直接的であれ、間接的であれ、ICS が関連するセキュリティインシデントが発生した場合は、インシデント対応におけるすべての活動において必ずしも「制御系 SIRT」が対応の主体になるとは限らない。
先述した「セーフティ」の確保等、発生事象における影響を鑑みた対応が必要であり、セーフティを確保するための判断や対応は、それらの知見を有する担当に任せる方が適切であり、同担当が適切な判断を行えるように、サイバーセキュリティの観点から支援を行うことが望ましい。この場合、対応を中心的に担う、いわゆる「旗振り」役ではなく、事象発生の要因にサイバー要素があるかを事中または事後に調査して、インシデントの解明を支援する役回りが想定される。
以上から、同 SIRT がどのような役割を担うかはインシデントの内容（現象、影響等）による。
なお、ICS 関連のセキュリティインシデントにおいて留意すべき観点には、「セーフティ」の他に、「ICS セキュリティ担当者コミュニティー」における検討では、事業者の事業の性質によって、製品の品質保証（Quality）、環境保護（Environment）、衛生管理（Health）等についても考慮した対応が求められることも分かり、それらの担当との平時からの連携も重要である。

3.2.2.2. 製造業における ICS 特有事象のモニタリングと早期検知

ICS 関連のインシデントの事象は、ランサムウェア感染のように脅迫メッセージが感染端末のモニターに表示されるような目に見える事象でサイバー要因だと判別し得る事象もあり得るが、ICS 特有の事象の中には、一見しただけでサイバー要因と判別することが難しい事象もあり得る。こうした ICS 特有の事象の中で、「制御系 SIRT」は、いち早くサイバー要因によって発生したものを検知・把握する能力を求められる。
しかし、これまでの ICS 関連の被害事案から推定できるサイバー要因の「ICS 特有事象」は限定的なため、上述のコミュニティーで、実際に感染があった事例も交えて、どのような「ICS 特有事象」はサイバー要因でも起き得るのかの机上検討を行った。検討結果から、サイバー要因を想定して報告対象としておくべき「ICS 特有事象」およびその報告基準や報告先について、これまでに JPCERT/CC で整理した内容を記載する。

- 報告対象とすべき製造業における「ICS 特有事象」とその例

製造業における ICS 関連のセキュリティインシデント事象は、機器故障等の一見サイバー要因によるものなのか不明なもの等、ICS 特有の環境で発生するものも想定しておくべきであり、そうした点を踏まえて、これまでに上述の「ICS セキュリティ担当者コミュニティー」で検討した「サイバー要因の可能性を想定しておくべき事象例」を次に挙げる。製造業における ICS 関連のセキュリティインシデントをいち早く発見して、組織内での早期の認識合わせと迅速な対処を行えるよう、これらの事象を報告対象に加える等のインシデント対応体制を整えるための参考としていただきたい。

■ サイバー要因が想定される製造業における ICS 特有事象の例

（ア）制御機器の異常検知（パラメーターの異常な値の表示等）
（イ）制御機器自体の動作遅延（HMI の応答が遅い等）
（ウ）制御機器の故障（機器の一部の損傷等、交換が必要な事態）
（エ）製品の不良率の増加（品質基準を満たさない製品の増加等）
（オ）工場の PC や HMI／SCADA 等の画面に不自然な表示（身代金要求等）

この他に、次のような場合も、工場関係者と協力して、サイバー要因の可能性も視野に早期に認識できる対象とすべきである。

（カ）原因が物理損傷等でなく、かつ原因特定が不明確な事象
（キ）複数箇所で何らかの事象が同時多発する場合
（ク）同一事象が任意の期間で頻発する場合

➢ 報告基準

前項では「サイバー要因が想定される製造業における ICS 特有事象の例」を記載したが、これらを適切なタイミングで把握するためには、「どのような事象が対象なのか」「どのタイミングで報告するのか」等のいわゆる「報告するための基準」を策定し、これらの事象に接する可能性がある組織内の関係者に周知しておく必要がある。
「報告するための基準」の策定と、組織内の関係者への周知は、「制御系 SIRT」の「検知能力」を備えるのに必要な要件である。

しかし、上記の「報告するための基準」を策定して組織内の関係者に周知し、実効性のある運用とすることは容易ではない。
そこで、JPCERT/CC が本書執筆時点で把握している上記の事象を適切なタイミングで把握するための取り組みについて、いくつかの組織での事例を紹介する。取り組んでいる各組織は、主に、「ある程度製造現場側で報告対象の事象を選別してから報告する事前フィルタリング方式（フィルリングあり）」と「製造現場側で報告対象の事象を一切選別せずに報告する全数報告方式（フィルタリングなし）」のいずれかを採用してトライ＆エラーを繰り返し、その取り組み結果をもとに、「報告するための基準」を策定することに取り組んでいる。そのため、試行錯誤をしながらの取り組みであることに留意し、参考としていただきたい。

取り組み例１）製造現場関係者側での報告前フィルタリング（対象事象選別）ありの場合

報告対象：（ア）から（エ）の中で（カ）、（キ）、（ク）の一部または全部に該当するケース、（オ）のケース 良い点：特定条件下の報告対象の選別効果の期待、不要な報告対象の削減効果の期待、報告者および報告を受ける者の工数削減 課題点：現場関係者での判断により報告すべき事象が報告されない可能性、現場関係者では特定条件の事象しか注意が払われなくなる可能性

取り組み例２）製造現場関係者側での報告前フィルタリング（対象事象選別）なしの場合

報告対象：（ア）から（オ）のすべてのケース、（カ）、（キ）、（ク）の一部または全部に該当するケース、その他の判断に迷うすべてのケース 良い点：報告対象の現場での誤った選別の低減効果の期待、「報告するための基準」を検討するための取り組み効果に関するデータをより的確に得られる期待 課題点：不要な報告対象の報告件数の増加、不要な報告対象における報告者および報告を受ける者の対応工数の増加

- 報告先（製造業における「制御系 SIRT」担当者が各事象を把握するための留意点）

前項の例を含む「サイバー要因が想定される製造業における ICS 特有事象」を把握するには、一見、サイバー要因か分からないため、報告や相談を待つだけでは SIRT へ対象事象が届かない場合があり得る。そのため、能動的に同事象の情報を入手するよう活動する必要がある。そこで、サイバー要因の可能性がある「ICS 特有事象」を入手するルートを、上述のコミュニティーで検討した。検討結果から想定されるルートのイメージは、次のようなものである。（図 7 参照）
なお、アからクの事案以外に、外部からの連絡によって認識する事案も想定されるため、それらも含めたイメージ図である。イメージ図では便宜的に「ICS のセキュリティ担当者（制御系 SIRT）」を中心に描がいているが、ICS 関連のセキュリティインシデント対応の中心的な役割（旗振り役）を意味しているわけではない。中心的な役割（旗振り役）を担うかは案件の性質にも寄るため、すべての案件で中心的な役割を担うとは限らない点に留意いただきたい。

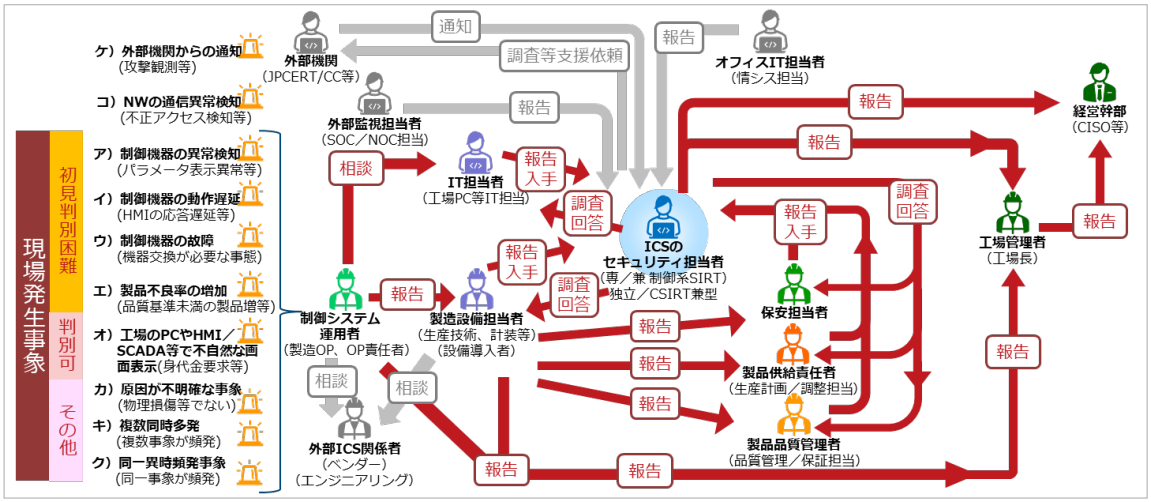

図 7　ICS のセキュリティ担当（「制御系 SIRT」）の各事象把握と関係者対応のイメージ
（SIRT 担当者のヒアリング等をベースに JPCERT/CC が作成）

3.2.2.3.　インシデントレスポンス時に必要な支援

発生事象とその影響にも寄るが、ICS 関連のインシデント対処では、次の対応を求められる場合がある。このため、それぞれの支援が行える能力も求められる要件である。
なお、各支援の記載順は優先度を示すものではない。

- 安全確保を最優先にした対応支援

プラント等の設備を有する事業者では、有事の際、エンジニアリングワークステーション（EWS）が被害にあっても、DCS や HMI、プラントの稼働を監視、制御している箇所への影響の把握と対応の検討が優先される場合がある。これは、安全確保を最優先にするためであり、稼働継続の是非や安全な停止措置等を検討して必要な措置を行い、その上で EWS 等への対応を行うこととなる。このとき、「制御系 SIRT」は製造現場関係者における安全確保のためのアクションを適切に判断する材料（セキュリティ観点での調査結果や影響等）を与える役割を担うことが想定される。
こうした安全確保等を最優先とした対応は、いわゆるファクトリーオートメーション（FA）工場においても同様であり、「制御系 SIRT」の役割も同様の視点での支援が想定される。

- 現地調査対応支援

発生事象によっては現地でなければ確認や調査ができないケースがあり、SIRT 関係者が現地対応する場合がある（現地でしかアクセスできない製造設備における調査や影響確認を行う必要があるケース、製造現場のネットワーク構成がオフィスネットワークと異なり、一部で独自の構築や運用をしているケース等）。

例えば、ネットワーク構成がフラットで、かつその接続先管理が出来ていないために通信経路の遮断の判断が容易でなく現場確認と対処が必要になったケースや、ネットワーク上の脆弱な端末の再感染対処を苦心して現場対応を行ったケースがある。
本調査が行われるのは、事中もあり得るが、事後調査となることが想定される。
なお、製造業の業種によっては危険物を取り扱う設備にも制御システムが使用されること等があり、発生した事象や被害対象設備等によっては人が近づいても問題無いのか事前に確認を要することも想定される。このため、SIRT 関係者による現地調査を行う場合は、現地の安全が確保されているかを事前に確認した上で行う必要がある。

- ICS 系ネットワークの通信遮断の要否判断支援

ICS 系ネットワークの通信遮断（論理的閉鎖、物理的閉鎖等）は遮断影響を想定して、遮断可能なところとそうでないところを事前に確認して有事の通信遮断の対応の参考とする必要がある。
ICS 系ネットワークの通信遮断は、ICS の正常稼働に必要な情報の流通を妨げる可能性があり、運用に必要な情報が提供されないと稼働継続や停止等の製造現場要員における運用判断を困難にしたり、フィールド機器の動作に影響を与えるといった思わぬ事態を引き起こす可能性がある。このため、オフィス系ネットワークに比べて、通信遮断を行うかは、より慎重に対応する必要があり、適切な判断を製造現場関係者（工場管理者、製品供給責任者、製造設備担当者等）が行えるよう、セキュリティ観点での影響を「制御系 SIRT」が SOC 等と連携して検討し助言等の支援を行う必要がある。

- 製造設備を停止した場合の操業再開プロセスにおける対応支援

安全確保等のセキュリティ以外の要素を優先して停止を行っていた場合、感染したマルウェアの駆除等のセキュリティ対応が十分でない場合がある。そのため、再発防止の観点から、停止した製造設備の操業再開の際、セキュリティ上の問題の解消有無を確認して、製造現場関係者へ報告し、操業再開判断を支援する役割を担うことが想定される。
なお、操業再開時または事後において、セキュリティ観点での再発防止策を提示して、保安等のさまざまな製造現場関係者とともに「安全性確保やその他の ICS 運用事情等を勘案した再発防止策」を検討し実装していくことが重要である。

3.2.2.4. リスクコミュニケーションにおいて必要な対応

「制御系 SIRT」の機能は CSIRT に包含されるケースの他、別組織として設置されるケース等があるが、いずれも CSIRT と連携して活動することが想定される。また、一般に、CSIRT には組織内外との情報のやり取りを行う「窓口」としての役割がある。

➢ 「窓口」の統合による情報流通の適正化と一体的な組織対応へ

「制御系 SIRT」の活動に関する情報の組織内外とのやり取りにおいても CSIRT と連携して組織として一体的にやり取りを行うことで、情報の流通をコントロールすることができ、情報の錯綜等の混乱を低減できる。また、事態の把握もしやすくなるといったメリットもある。このため、「制御系 SIRT」が単独で組織内外との窓口になるのではなく、CSIRT と連携した「窓口」の設置が有効である。なお、実務的な視点での組織内外のやり取りにおいては、「制御系 SIRT」が、直接、組織内外の関係者とコンタクトを取る方が、仲介者が少なく情報の齟齬を減らして迅速なアクションとなる面もあることから、「制御系 SIRT」の活動内容次第では、必ずしも CSIRT 経由である必要は無いことも補足しておく。

3.2.3. インシデントマネジメントおよびハンドリングに資する外部組織との連携

本項では、ICS を考慮したインシデントマネジメントおよびインシデントハンドリングを行う上で、それぞれの機能の強化等に資する外部組織との連携について述べる。
外部組織との連携とひと口に言っても、連携する組織に応じて、さまざまな連携が想定される。ICS 関連のインシデント対応における連携を念頭に、可能な限り、具体的に連携イメージをつかんでいただくためにも、ここでは、JPCERT/CC との連携を想定して述べる。上述のコミュニティーでこれまでに取り組んで来たことをベースに、「有事に備えた外部組織との脆弱性対応における連携」「有事における外部組織との迅速な情報連携」の 2 点について、「制御系 SIRT」の活動ポイントを記載する。外部連携の参考としていただきたい。

3.2.3.1. 「制御系 SIRT」が有事に備えて活用しておくべき脆弱性対応における外部連携

① ICS 関連の脆弱性情報を迅速かつ適切に入手できる外部ソースの確保

脆弱性はサイバー攻撃を成立させてしまう要因の一つであり、可能な限り早期に解消を行うことが望ましい。仮に解消するような対策が打てなかった場合でも、代替策を講じる等でインシデントの未然防止や被害時の影響度の低減といった効果が期待できるため、脆弱性情報の把握とその対応は、有事に備えて行うべき「制御系 SIRT」の重要な活動である。
ICS 関連製品の脆弱性情報をタイムリーに入手するには、次の脆弱性情報を提供するサービスを利用することが有効である

Japan Vulnerability Notes（JVN：脆弱性対策情報ポータルサイト）
https://jvn.jp/
※RSS 配信も行っており、タイムリーな情報入手に活用できる

② ICS 関連の脆弱性情報の組織内ハンドリングとその結果の JPCERT/CC へのフィードバック

➢ 組織内ハンドリング

ICS 関連の脆弱性情報を入手すると、先述の「脆弱性の管理と対応」で述べたように、資産管理表との突合等を行って自組織で対応すべきものかの判断を行い、対応すべきものがあれば、上述の「脆弱性に関する 3 つの対応方針」を検討して必要な対策を講じることになる。

➢ JPCERT/CC へのフィードバックと「制御系 SIRT」活動のサイクル化

JPCERT/CC による脆弱性情報の提供は、本書で対象とする「制御系 SIRT」において、ぜひ活用していただき、インシデントの未然防止や有事の際の被害低減につなげていただきたいと考えている。しかし、提供した脆弱性情報がどのように活用されているのか分からないため、JPCERT/CC では「制御系 SIRT」における活用を想定した最適な提供形式や提供項目等となるような見直しおよびフォローアップを、本書執筆時点で、これまで十分に行えていなかった。一方で、「制御系 SIRT」の構築や運用改善に取り組む組織が徐々に増えつつある現状を鑑み、「制御系 SIRT」への脆弱性対応のフォローアップがより必要になって来ることが想定される。そのため、JPCERT/CC では、脆弱性情報の活用に関する「制御系 SIRT」からのフィードバックを期待している。実際、「脆弱性の管理と対応」の項目で述べた資産管理表との突合は、ICS 関連の脆弱性情報を JPCERT/CC から入手している ICS ユーザー組織のセキュリティ担当者からいただいたフィードバックを参考に、脆弱性情報をより活用いただくための活用術として整理したものである。
「制御系 SIRT」による ICS 関連の脆弱性情報の活用をより効果的に支援していくため、「制御系 SIRT」および準ずる担当者からのさまざまなフィードバックを JPCERT/CC では期待している。
次にフィードバックしていただきたい例を記載する。参考としていただきたい。

■ 「制御系 SIRT」から JPCERT/CC へいただきたい脆弱性情報の活用におけるフィードバック例
- ➢ 該当する ICS 製品の利用有無
- ➢ 該当する脆弱性の対応要否の判断結果とその理由
- ➢ 該当する脆弱性の対策（根本対処、ワークアラウンド対応等）
- ➢ 脆弱性情報の提供形式（提供ツール、電子データ形式等）
- ➢ 現行の脆弱性情報には無いが対策のために必要と考える追加情報

「制御系 SIRT」が平時から行うべき活動には種々あるが、脆弱性対応もその一つであることは先に述べたとおりである。特に ICS 関連の脆弱性対応は、一般にパッチ適用が容易でない等のさまざまな事情を抱えており、その対応は容易ではない。しかし、ICS が直接的または間接的に影響を受けるセキュリティインシデントは今後も発生する可能性があり、「制御系 SIRT」による ICS 関連の脆弱性対応は避けては通れない課題である。
このため、ICS 関連の脆弱性対応におけるフィードバック等を通じて JPCERT/CC との外部連携を平時から行うことは、脆弱性に対する「共同対応」ともなることから、より効果的な脆弱性対応を進めるこ

とができるようになると考えられる。つまり、情報の流れ方は、必ずしも JPCERT/CC から「制御系 SIRT」（ICS ユーザー組織側）へと向かうだけではないことがわかる。こうした「連携」の関係性は、「制御系 SIRT」の活動目的を意識させ、活動の停滞を起きにくくする効果も期待できる。

3.2.3.2. 「制御系 SIRT」が有事において外部組織と適切に情報連携を行うために必要なこと

① 平時からの相談や調査依頼等が可能な連絡先の確保と「共同調査」の価値の組織内文化形成

➢ 平時からの相談や調査依頼等が可能な連絡先の確保

ICS 関連のセキュリティインシデントについて、実務を担う SIRT のオペレーションレベルでの相談先を確保しておく必要がある。特に、公的な組織の担当窓口を確保し、その担当と日ごろから情報交換ができる状態にしておくことで、平時から自組織で留意すべき情報を獲得でき、有事の際の迅速な対処のための情報の連携につながる。なお、リスクコミュニケーションでも述べたように、窓口は組織内 CSIRT と連携して行うことが効果的である。そのため、外部組織との連携は、CSIRT 経由もしくは CSIRT にも共有しつつ行うことも検討しておく必要がある。

➢ 情報連携による「共同調査」の価値と組織内におけるその文化形成

外部組織へセキュリティインシデントに関する情報を共有する際に、いくつかのハードルが存在することが分かっている。
「制御系 SIRT」関係者との取り組みの中で、主に、「共有することの意義や価値の理解不足」「インシデント関連情報の流出等による事業影響の懸念」が挙げられる。
前者については、その意義や価値を十分伝えることができていない現状がある。JPCERT/CC においては、共有や報告をいただいた組織には、その対応結果を可能な限りお伝えしているが、今後も共有組織に報告するだけでなく、こうした連携の価値を広くアナウンスしていく必要があるものと思われる。一方、「制御系 SIRT」においては、情報を共有することで「調査すべき箇所の見落としの低減」「他の被害事案からの調査すべき情報の追加入手」等といった自組織における調査の向上に資するだけでなく、JPCERT/CC を介した他組織や産業界への（匿名化された状態での）情報共有ともなって、二次被害防止に貢献することとなる。さらには、類似事案が発生していた場合の共通的な脅威（共通した C&C サーバーが設置された IT インフラ、悪用された ICS 関連製品の脆弱性等）への JPCERT/CC による調整および追加の情報収集や分析等に資するため、結果的に ICS 関連のインシデント対応支援に間接的に協力することとなり、産業界の ICS セキュリティの向上に貢献することにもつながる。

➢ 「共同調査」の価値の組織内文化形成

つまり、報告組織と外部組織（この場合、JPCERT/CC を指す）が協力し合うことで、効果的なインシデントの調査が可能となり、いわゆる「共同調査」の価値を双方で享受できることとなる。「共同調査」の意義や価値を組織内に伝えて行くには、自組織での ICS に関するインシデント対応訓練等において、こうした情報連携を日ごろから入れ込んで取り組むことも一案である。

後者については、インシデント関連情報を外部共有することで部外者への流出等に発展し事業影響とならないかといったこと等、以前から、外部共有することへの一定の懸念を事業者側が有している。こうした懸念は、単に共有先との信頼度に任せて共有の可否を判断するだけでなく、共有すべき情報とそうでない情報を事前に理解しておくことで、一定の解消が可能である。詳細は②で述べる。

② 外部共有可能な情報の整理と共有方法の平時からの認識合わせ（有事における外部連携の準備）

➢ 外部共有可能な情報の整理

前項で述べた「インシデント関連情報」の外部共有における事業者側の懸念を一定程度解消するには、「調査に必要で外部共有が可能な情報」とそうでない情報に区別する必要があり、これらの備えを平時から行っておくことが重要である。ここでいう「(被害にあった疑いを含む）被害組織からみた、調査に必要で外部共有が可能な情報」とは、共有した情報によって組織は特定されないが、インシデント調査等に必要な最低限の情報を指す。次に ICS 観点からみたその例を挙げる。事前準備の参考としていただきたい。

■ インシデント調査に必要な外部共有情報の例（JPCERT/CC へ共有する場合）
- ✓ ICS に直接的・間接的な影響が想定される不審な通信情報
  （例：ICS へのリモートアクセスの通信ログ等）
- ✓ ICS に直接的・間接的な影響があるマルウェア情報
  （例：ICS 機器が感染または ICS 監視機器で検知した検体に関する情報等）
- ✓ ICS に直接的・間接的な影響があるその他攻撃手法に関する情報
  （例：事案に関連する可能性があるフィッシングメール情報等）
- ✓ 直接的・間接的に影響を受けた ICS 関連の情報
  （例：生産設備の監視システム、影響があった ICS のネットワーク構成図に関する情報等）
- ✓ 影響を受けた ICS において想定される被害要因の情報
  （例：脆弱性の有無等）

参考までに、上記の情報を共有いただくことで可能となる調査の一例を以下に示す

■ 上記の情報による依頼で JPCERT/CC が調査を行う場合（一例）
- — 不審な通信元/先の特定（不審なインフラの停止等の調整等も行う場合あり）
- — 検体のソースや挙動等の分析による動作目的や感染対象における具体的な被害内容（窃取された情報の範囲等）の推定等
- — ICS に直接的・間接的な影響を与えた感染経路の推定
- — 脆弱性情報と申告いただいた被害事案との関連性の推定
- — 他の被害事案との関連性の有無や比較検討による追加調査箇所の有無の確認
- — これらの分析結果による攻撃の流れの推定

なお、ICS に関するインシデントおよびその疑いに関する調査の JPCERT/CC への依頼の詳細は、次の Web ページを参照いただきたい。

- インシデント対応依頼
  https://www.jpcert.or.jp/form/
- 制御システムインシデント対応依頼
  https://www.jpcert.or.jp/ics/ics-form.html

➢ 外部共有方法の平時からの認識合わせ

上記のように外部共有可能な情報を整理した上で、有事の際に連携が想定される外部組織と共有方法等について認識合わせをしておくとより良い。平時からの認識合わせができていると、共有された情報を適切に双方で取り扱い、迅速な連携が可能となる。

図 8　「制御系 SIRT」と JPCERT/CC 間の情報連携イメージ

ICS セキュリティの情報連携において、「制御系 SIRT」（ICS ユーザー組織）と JPCERT/CC の関係は、一般に、情報の受領者と提供者のように思われがちだが、サイバーセキュリティは協力しあうことで成り立つ世界であり、情報の流れも JPCERT/CC が必ずしも情報提供者という一方通行ばかりではない。外部連携は、「制御系 SIRT」にとっても、連携する外部組織（この場合 JPCERT/CC を指す）にとっても有益だといえる。

4. まとめ

本書は、巻頭で述べたように、「制御系 SIRT」の構築に必要な要件の検討にあたって、手がかりが少なく暗中模索となっている製造業における ICS セキュリティ担当者に対して、適切な機能を備えるための要件検討の参考となる情報を提供すべく、ICS セキュリティ担当者コミュニティー等を通じて検討した取り組みのうち、共有可能な知見をまとめたものである。このため、記載した知見は、ICS セキュリティに取り組んでいるまたは取り組まなければならない実務者と JPCERT/CC が連携して検討して来たものであり、より実践的な知見を掲載している。

しかし、検討すべき「制御系 SIRT」に関する要件はまだまだあり、網羅的に検討と本書への掲載が出来ているわけではない。また、「制御系 SIRT」を取り巻く諸条件（業種の特性、対象設備の特性や新技術の導入等）の変化により「制御系 SIRT」に求められる機能等も変わって来る可能性がある。このため、本書の活用にあたっては、必要に応じて、その内容が加筆修正される可能性がある点に留意いただきたい。

本書に掲載の内容はあくまで参考情報であり、各要件等、記載した内容がすべての製造業の ICS セキュリティ担当者およびその関係者に適した解答を与えるものでないが、「制御系 SIRT」またはそのような機能を備えるにあたり、何かしらの知見を提供するものであり、求められる機能の適切な構築を支援するものである。

最後に、ICS セキュリティのすべてのステークホルダー、特に「制御系 SIRT」の構築や運用に取り組む製造業の ICS セキュリティ担当者のみなさまへのお願いです。本書を活用されましたら、フィードバックをお願いいたします。本書の改善等、今後の支援活動の参考といたします。

5. 謝辞

本書は、ICS セキュリティ担当者コミュニティーメンバー（延べ 35 名以上の製造業の ICS セキュリティ担当者）、越島一郎名誉教授（名古屋工業大学）、橋本芳宏名誉教授（名古屋工業大学）、その他の ICS セキュリティに関わる関係者のご協力により、作成されました。ご協力いただいたみなさまへ感謝申し上げます。

Appendix 1.　　用語解説

本書で使用された用語の一覧です。

No	用語	解説
1	ICS	Industrial Control System（産業用制御システム）
2	SIRT	Security Incident Response Team（セキュリティインシデント対応チームやその体制）
3	CSIRT	Computer Security Incident Response Team コンピューターセキュリティインシデントに対応するチーム 主に情報システムにおけるセキュリティインシデントに対応する体制として用いられる 特段の説明が無い限り本書ではこの意味で使用
4	制御系 SIRT	本書では、制御システムを対象とする SIRT 機能を指す用語として使用している。なお、同様の意味の用語として OT-SIRT、FSIRT 等が使用される場合があるが、 制御システムを対応範囲とするインシデント対応体制についての統一的に使用される確立された呼称はまだないと承知している なお、制御系 SIRT は物理的に CSIRT と別組織である必要は無く、本書ではあくまで、制御システムのさまざまな事情を勘案した活動が可能な「機能」という意味あいで使用している
5	インシデント	制御システムの運用におけるセキュリティ上の問題として捉えられる事象 特段の説明が無い限り本書ではこの意味で使用

Appendix 2. 参考文献

- 経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き第 2 版」
  https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf
- FIRST「 Computer Security Incident Response Team (CSIRT) Services Framework」
  https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_ja.pdf
- JPCERT/CC「CSIRT マテリアル」
  https://www.jpcert.or.jp/csirt_material/
- National Cyber Security Division「推奨プラクティス：工業用制御システムにおけるサイバーセキュリティインシデント対応能力の開発」
  https://www.jpcert.or.jp/research/2010/CSincident_response_20100330.pdf
- Homeland Security「Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability」
  https://www.cisa.gov/sites/default/files/2023-01/final-RP_ics_cybersecurity_incident_response_100609.pdf
- Tomomi Aoyama, Kenji Watanabe, Ichiro Koshijima, and Yoshihiro Hashimoto 「Developing_a_Cyber_Incident_Communication_Management_Exercise_for_CI_Stakeholders」
  https://www.researchgate.net/publication/321199356_Developing_a_Cyber_Incident_Communication_Management_Exercise_for_CI_Stakeholders
- 独立行政法人情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラム 3 期生 資産管理プロジェクトメンバー「制御システムにおける資産管理ガイドライン」
  https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2020/ngi93u0000002jlf-att/000083594.pdf
- DRAGOS「Improving ICS/OT Security Perimeters with Network Segmentation」
  https://www.dragos.com/blog/improving-ics-ot-security-perimeters-with-network-segmentation/
- SANS「The Purdue Model and Best Practices for Secure ICS Architectures」
  https://www.sans.org/blog/introduction-to-ics-security-part-2/
- Zscaler「ICS セキュリティの Purdue モデルとは」
  https://www.zscaler.jp/resources/security-terms-glossary/what-is-purdue-model-ics-security
- サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会「サイバー攻撃被害に係る情報の共有・公表ガイダンス」
  https://www.meti.go.jp/press/2022/03/20230308006/20230308006-2.pdf

変更履歴

公表日	版	変更概要
2024-03-27	Ver.1.0	初版作成