Japan Computer Emergency Response Team Coordination Center



JPCERT CC®

# 制御システムセキュリティ

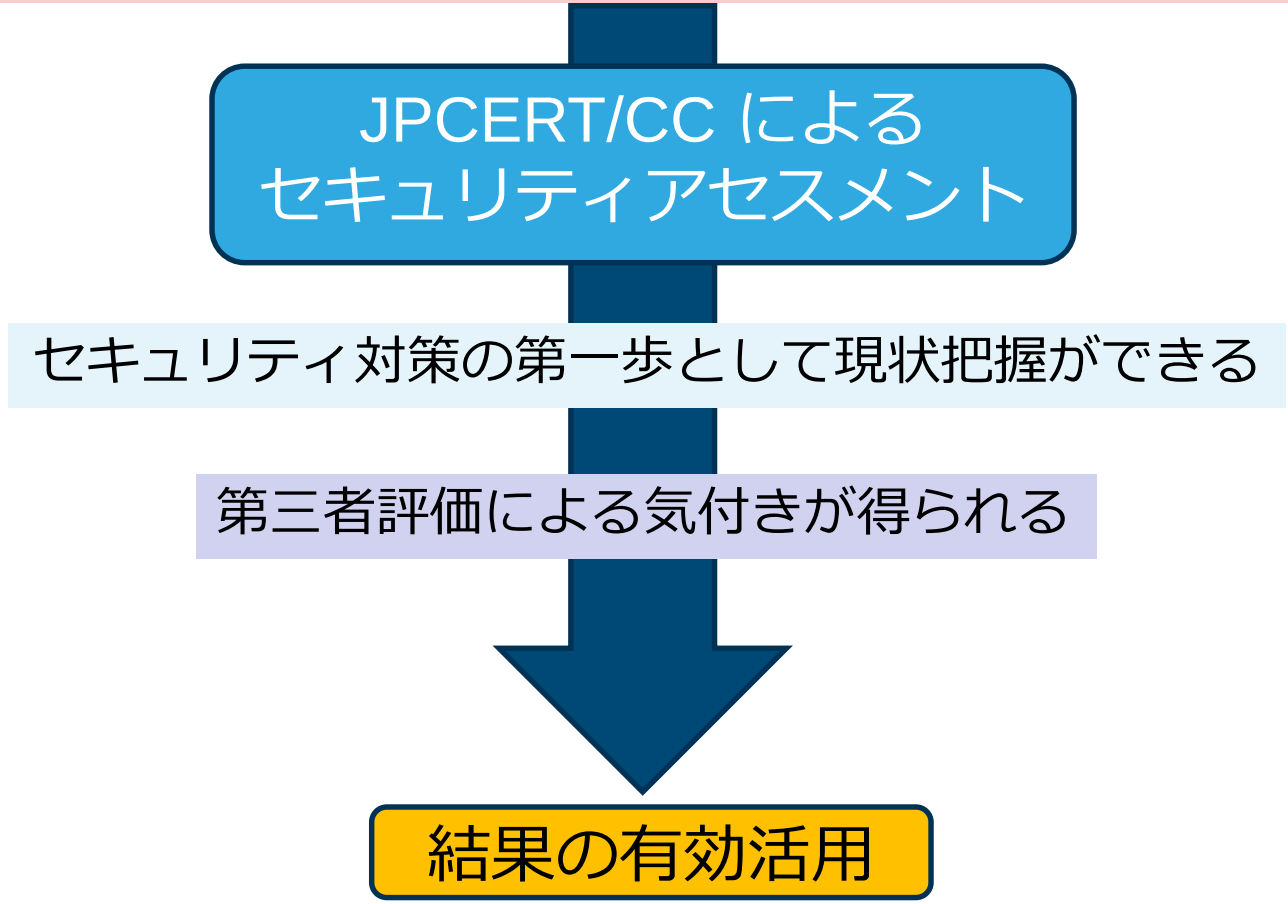
# アセスメントサービス

一般社団法人JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ

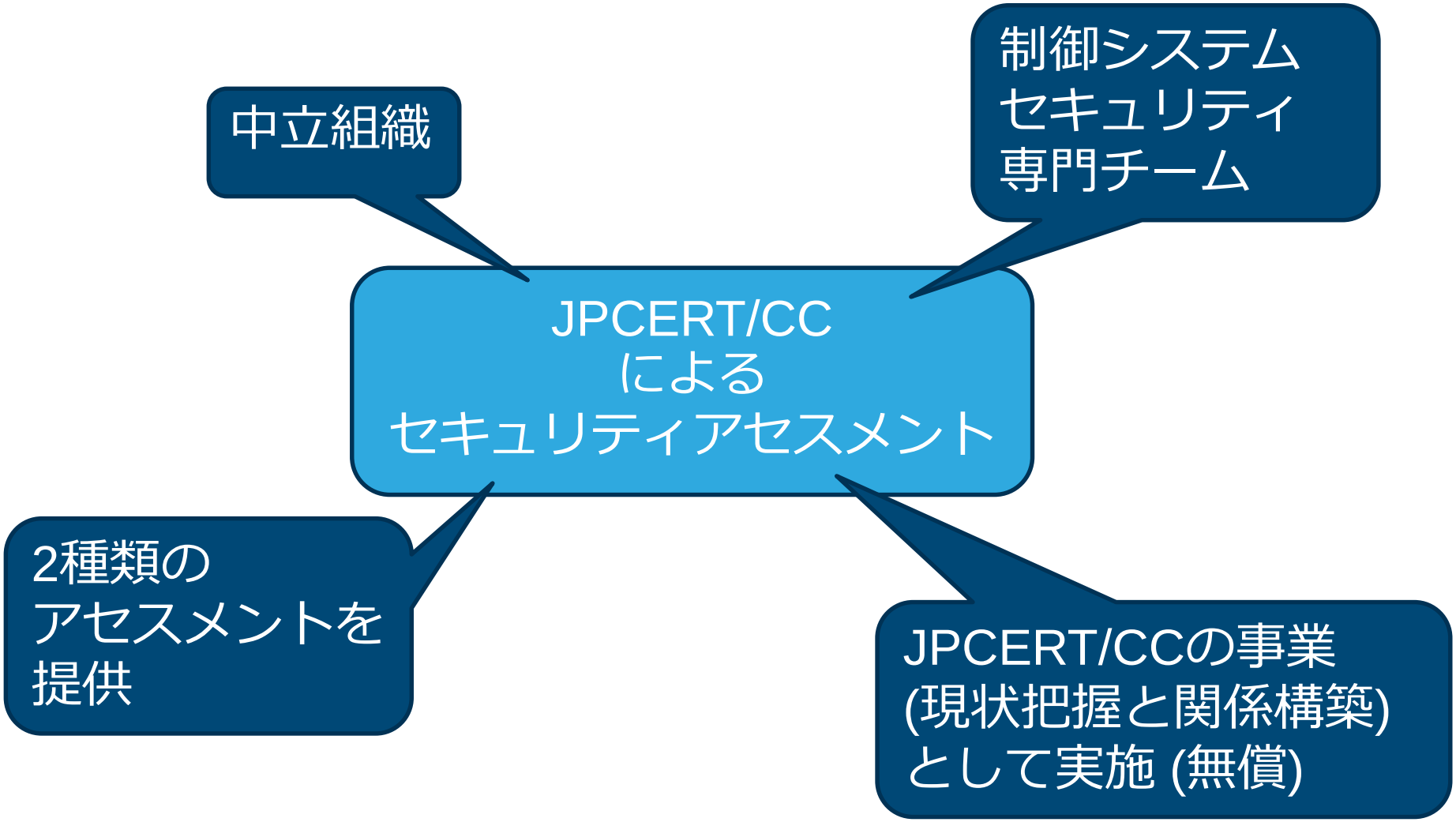
# 目次

# はじめに：メリット その１

制御システムのセキュリティ、何から手をつけたらいいのか分からない
現状把握の必要性はわかるが、評価時間があまりかけられない



# はじめに：メリット その２



# 背景

- アセスメント実施の背景

サイバーセキュリティ対策の第一歩として、アセスメント実施の必要性が言われています。アセスメントにより、組織の現状を把握し、明らかになったリスクを評価することにより、必要な対策を検討することが可能になります。
JPCERT/CCでは自己評価ツール（日本版SSAT, J-CLICS）を提供していますが、第三者による評価を行うことにより、自己評価では得られない気付きを得ることができます。
このため、JPCERT/CC によるオンサイトのアセスメントをご提案いたします。

日本版SSAT (SCADA Self Assessment Tool)
https://www.jpcert.or.jp/ics/ssat.html
J-CLICS (Check List for Industrial Control Systems of Japan)
https://www.jpcert.or.jp/ics/jclics.html

# 概要

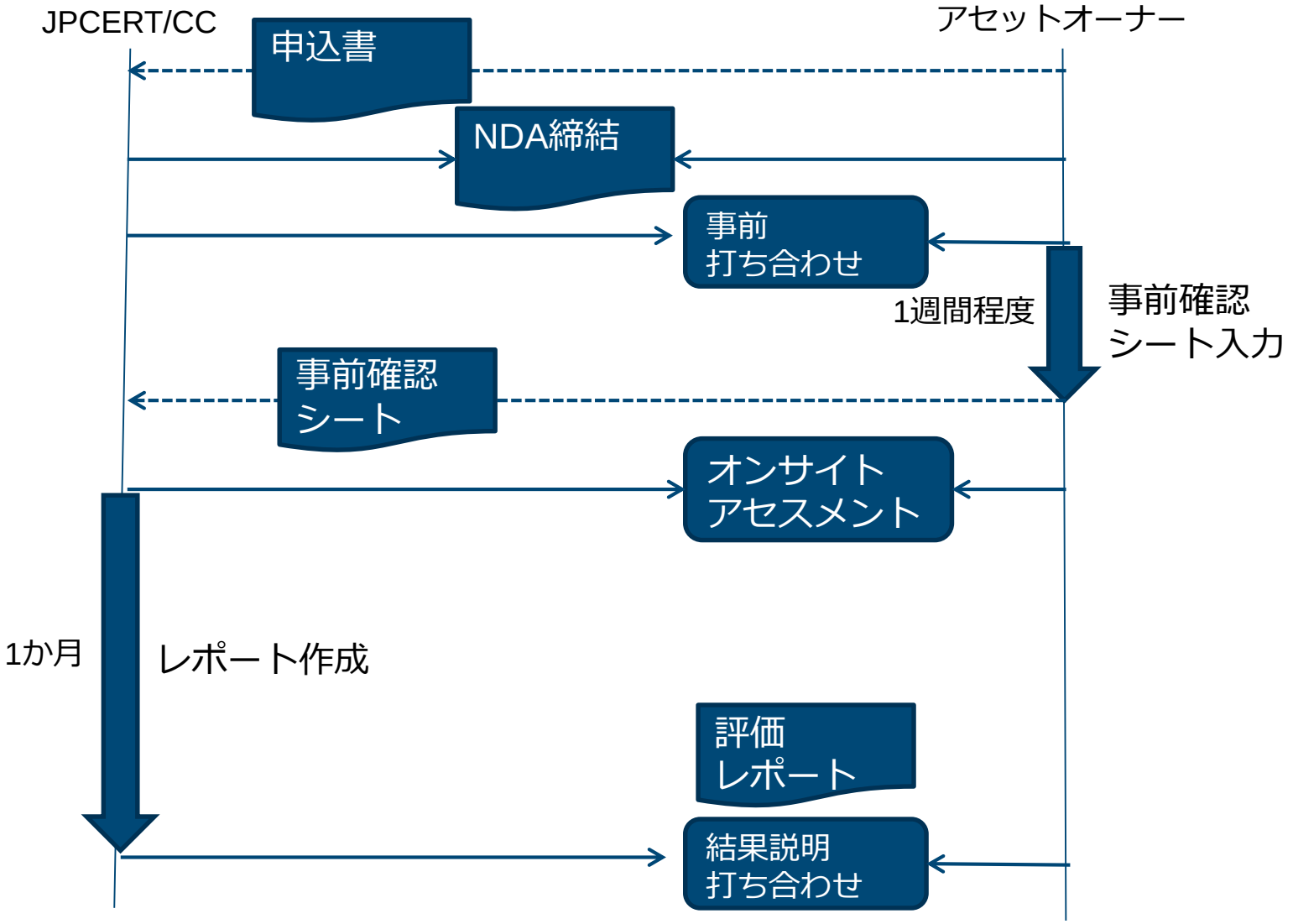
- ベースラインアプローチ
  英国政府のCPNI (Centre for the Protection of National Infrastructure) が開発したSSAT をベースに開発した日本版SSAT、または、制御システムセキュリティのガイドラインとして用いられる米国のNIST文書に基づいてアセスメントを行います
  ＊NIST: National Institute of Standard and Technology

- オンサイトアセスメント
  JPCERT/CCの担当者がアセットオーナーのサイトを訪れ、ヒアリングを行い、可能な範囲で証跡の確認を行います。
  その後、結果をまとめレポートとして提出します。

- 対象
  制御システムを利用されている国内のアセットオーナー様

- メリット
  現状のセキュリティの評価が行え、第3者評価による気付きを得ることができます。

# アセスメントの流れ



# アセスメントの流れ（詳細）

| | 事前打ち合わせ | 事前確認シート記入 | オンサイトアセスメント | レポート作成 |
|---|---|---|---|---|
| 所要時間 | 約2時間 | 約4時間 | 約8時間 | 1か月 |
| 内容 | ■アセスメント詳細説明<br>■事前確認シートの記入方法説明 | | ■オンサイトアセスメント<br>■証跡の確認<br>■ラップアップ会議 | ■スコア<br>■主要ポイントに対するコメント |
| アセットオーナー | ○ | ○ | ○ | |
| JPCERT/CC | ○ | | ○ | ○ |

# 2種類のアセスメントをご提供（SSATとTR）

SSATまたはTRのいずれかを選択いただきます。
SSAT：SCADA Self Assessment Tool
TR： Technical Review

導入から運用までの全般のアセスメントを行いたい場合はSSAT
ファイアウォールの設定内容等の技術面の詳細なアセスメントを
行いたい場合はTRを選択してください

| | SSAT | TR |
|---|---|---|
| アプローチ | ベースライン | ベースライン |
| 基準 | 日本版SSAT | NIST SP800-53<br>NIST SP800-82 |
| 分野 | 全般（デザイン、購買、導入、運用） | 技術的（設計、運用） |

NIST SP800-53 連邦政府情報システムにおける推奨セキュリティ管理策
NIST SP800-82 産業用制御システム(ICS)セキュリティガイド

# SSATベースのアセスメント（SSAT）

- 日本版SSATの項目に基づいてヒアリングを行い、JPCERT/CCが判定します。
- 可能な範囲で証跡の確認を行います
- 結果レポートとしては、SSATのスコア、および、主要項目に対するコメントになります
- サイトヒアリングは1日/1システム

# SSAT詳細

- リスクと脅威の理解
- 継続した統制の確立
- セキュア・アーキテクチャーの実装
- 意識とスキルの改善
- 対応能力の確立
- サード・パーティ・リスクの管理
- プロジェクト参画
- 調達

JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

安全・安心なIT社会のための、国内・国際連携を支援する

**1) 事業リスクの理解 (グッド・プラクティス・ガイド　プロセス・制御と SCADA セキュリティ - セクション 3.1 または ガイド 1 を参**

*事業リスクの要素は脅威、影響、脆弱性です。事業リスクをよく理解することで、初めて情報に基づいたセキュリティの適切なレベルはどのくらいか、改善すべき作業実施方法はどういったものかを判断できるようになります。*

**システムとビジネスリスクを理解する** (3.4.1 システムの理解; 3.4.2 事業リスクの評価)

| | | |
|---|---|---|
| 1 | 安全管理責任者はSCADA/遠隔監視ネットワークの棚卸監査と評価を実施し、最新の状態を管理していますか？（例: どんなシステムが存在しているか、機能は、重要な 業務/安全性は、設置場所は、所有者の明示、サポート担当者は誰か） | 一部 |
| 1a | 「はい」を選択したなら、それは過去12ケ月以内に見直し、監査結果報告書を作成していますか？ | いいえ |
| 2 | 安全管理責任者はシステムの事業リスクを、定められた手順に則って評価していますか？（例:リスクの発生の可能性と、リスクが発生した結果として予想できる影響でリスクを表します） | 一部 |

**脅威を理解する** (3.4.3 脅威の理解)

| | | |
|---|---|---|
| 3 | 安全管理責任者はSCADA/遠隔監視システムに起こりうる脅威を特定し、脅威評価に着手していますか？（例: DoS 攻撃、ネットワーク侵入、ウイルス、ワーム感染） | はい |
| 3a | 「はい」を選択したなら、それは過去12ケ月以内に見直していますか？ | いいえ |
| 4 | 安全管理責任者は特定のシナリオを考慮した、脅威評価に着手していますか？（例:特定のOSを搭載したコンピュータシステムにおける攻撃被害や障害、Ethernet/IP ネットワークにおける攻撃被害や障害など） | いいえ |
| 4a | 「はい」を選択したなら、それは過去12ケ月以内に見直していますか？ | いいえ |

**影響を理解する** (3.4.4 影響の理解)

| | | |
|---|---|---|
| 5 | 安全管理責任者はSCADA/遠隔監視システムで脅威が実際に起こった際の、プロセス制御システムへの影響と結果を文書化していますか？（例: ブランドへの影響、規定違反、業務目標の達成不能、財政上の損失） | いいえ |

# NIST ベースの技術的アセスメント（TR）

- アセスメント基準： NIST SP800-53 の技術項目、および、NIST SP800-82のガイドラインに基づいてヒアリングを行います
  - ネットワークの評価
  - セキュリティ対策の評価
  - ITとOTの連携状況
  - ベンダのサポート状況
  - モニタリング
- ネットワークアーキテクチャ図面などの確認を行います
- 結果レポートは、 各評価項目に基づくスコア、および、主要項目に対するコメントになります
- サイトヒアリングは1日/1システム

# TR 詳細

- NIST SP800-53 技術管理策
  - AC(20) アクセス制御(Access Control)
  - AU(11) 監査および責任追跡性(Audit and Accountability)
  - IA(7) 識別および認証(Identification and Authentication)
  - SC(23) システムおよび通信の保護(System and Communications Protection)
- NIST SP800-82
  - ネットワークアーキテクチャー
  - セキュリティ管理策

# 評価レポートイメージ

JPCERT CC®

## 制御システムセキュリティ
## アセスメントレポート

**基本情報**

御社名：
サイト：
システム名：
アセスメント実施日：

アセスメント手法：日本版 SSATによるオンサイトアセスメント

**アセスメント結果サマリー**

スコア（グッド・プラクティスの準拠率）

| | |
|---|---|
| 1) 事業リスクの理解 (10) | 2.5 |
| 1a) 脆弱性を理解する (10) | 2.5 |
| 2) 継続した統制の確立 (5) | 1.5 |
| 3) セキュア・アーキテクチャの実装 | |
| 周囲防御 (26) | 11 |
| マルウェア保護 (13) | 8.5 |
| 内部の脅威 (9) | 1 |
| セキュリティ管理 (3) | 2.5 |
| バックアップと回復 (3) | 1 |
| 物理的セキュリティ(6) | 5.5 |
| 4) 意識とスキルの改善 (5) | 0 |
| 5) 対応能力の確立 (5) | 0 |
| 6) サード・パーティ・リスクの管理 (16) | 6.5 |
| 7) プロジェクトへの参画 (4) | 0 |
| 8) 調達 (5) | 0 |
| 総合(120) | 42.5 |

緑はグッド・プラクティス推奨のスコアが85%以上であることを表します
橙はグッド・プラクティス推奨のスコアが60～84%であることを表します
赤はグッド・プラクティス推奨のスコアが59%以下であることを表します

**アセスメント結果詳細**

1) 事業リスクの理解
発見事項はありませんでいした。
2) 維続した統制の確立
発見事項はありませんでした。
3) セキュア・アーキテクチャの実装
ネットワークアーキテクチャ

| | |
|---|---|
| 発見事項 | １つの PC によるデュアルホーム接続により、制御ネットワーク上の２つのシステムが接続されていました。 |
| 懸念事象 | いずれか一方のシステムが侵害を受けた場合、容易にもう１つのシステムにも侵害が及ぶ可能性があります。 |
| 推奨対策 | ファイアウォールによるネットワークの隔離が望まれます。 |

4) 意識とスキルの改善

| | |
|---|---|
| 発見事項 | 注意喚起プログラム活動計画、セキュリティ技術を習得する計画・措置などが現状とくに存在していませんでした。 |
| 懸念事象 | 組織としての対応能力向上が見込まれません。 |
| 推奨対策 | 何らかの意識とスキル向上の施策が望まれます。 |

5) 対応能力の確立
発見事項はありませんでした。
6) サード・パーティ・リスクの管理
発見事項はありませんでした。
7) プロジェクトへの参画
発見事項はありませんでした。
8) 調達
発見事項はありませんでした。

**全体を通じた所感**

オフィスネットワークとの接続は無いとのことで、「Air Gap」の対策がなされていることが確認できました。しかし、「Air Gap」によって守られた制御ネットワークでもマルウエアに感染する事故が起こっています。ウイルス対策ソフトは一部導入されていますが、セキュリティパッチに関しても、定期メンテナンスのタイミング等で適用が推奨されます。

**（＊） 評価結果に関しては、匿名化および統計化して公開する場合があります**

# 申し込み方法、お問合せ先

別紙 申し込み書に記入の上、下記に送付ください

JPCERTコーディネーションセンター
制御システムセキュリティ対策グループ
—Email：icsr_reg@jpcert.or.jp

お問い合わせ先　担当：落合、中谷
—Email：icsr@jpcert.or.jp