『工場のインシデント対応訓練シナリオ』の実践から学ぶ

- 制御系SIRTを含む組織内関係者が取り組むべき実務的な訓練とは（訓練結果の分析の抜粋より）-

一般社団法人JPCERTコーディネーションセンター
国内コーディネーショングループ
制御システムセキュリティ シニアアナリスト
河野 一之

アジェンダ

1. 複数社による「訓練」結果の俯瞰的な分析の概要

2. 俯瞰的な分析で見られた特徴（抜粋）

a. 8社を俯瞰的に見た際に見られる特徴（良い点）
b. 8社を俯瞰的に見た際に見られる特徴（課題点）

3. トークセッション：見られた特徴を深掘り

1. 複数社による「訓練」結果の俯瞰的な分析の概要

『工場のインシデント対応訓練シナリオ』実践の参加概要

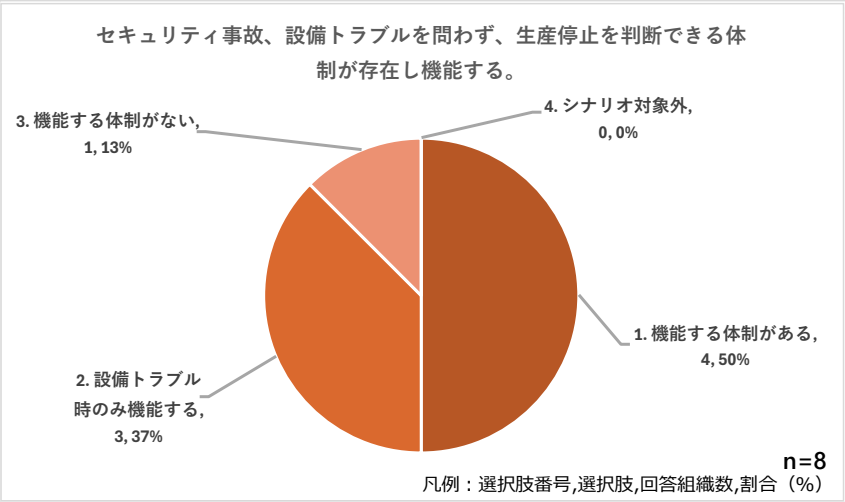
■ 『工場のインシデント対応訓練シナリオ』実践に関する参加概要は次のとおり

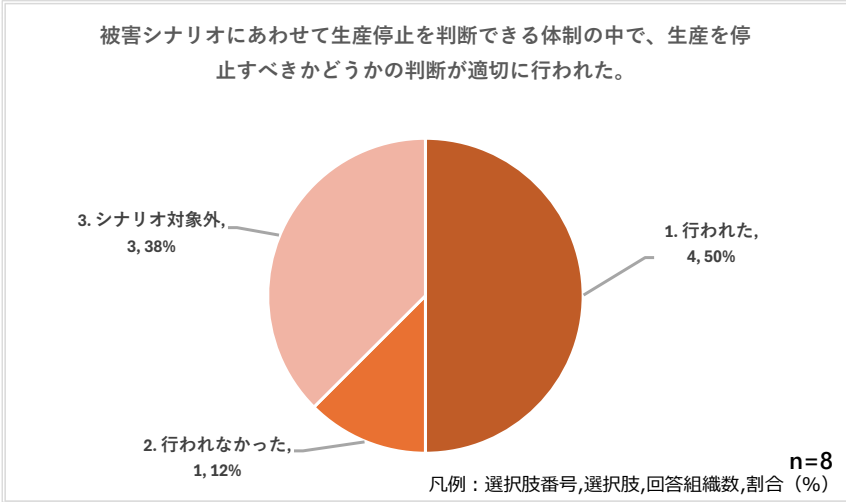
調査対象	ICSセキュリティ担当者コミュニティーにおける一般製造業 （化学、鉄鋼、電機・精密、医薬、自動車、機械等）
参加組織数	8社
評価項目数	全75項目
評価カテゴリー	1. 実装評価（全60項目：事前対策、訓練準備～事後対応までで、個々の対策・対応を評価） 2. 総合評価（全15項目：「日常的に取り組める」「訓練として取り組める」 「対処では外部組織と連携ができる」の3要素について評価）
調査手法	チェックリストによる評価

2. 俯瞰的な分析で見られた特徴（抜粋）

- a. 8社を俯瞰的に見た際に見られる特徴（良い点） -

工場関係者が参加して生産影響を想定

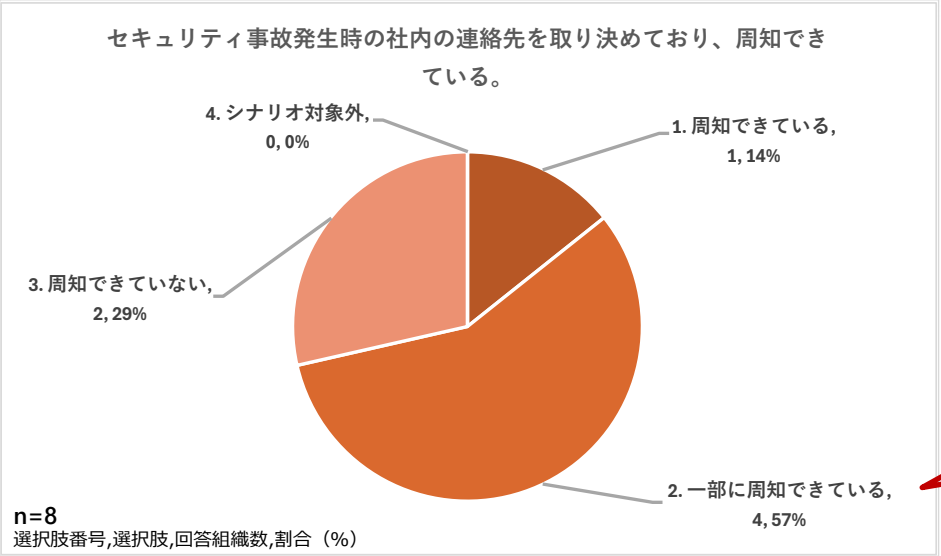




■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

- 工場関係者が参加し、「工場影響（生産停止判断等）」を想定した**体制の機能有無が確認**できた
- 工場関係者が参加していることで、生産停止等の**判断が「適切に」行われたとの確認**ができた

セキュリティ事故向けの連絡網が事前に整備されている



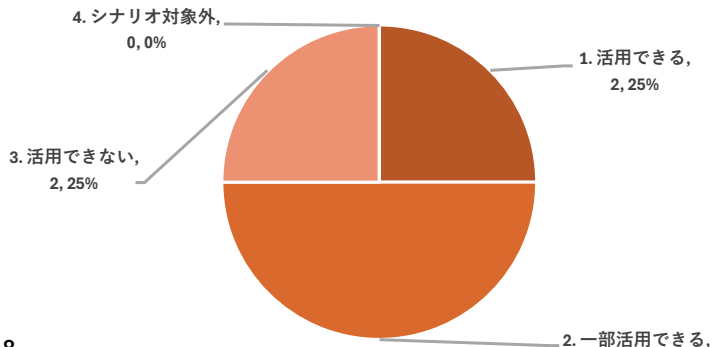
訓練を活用した「連絡網の周知や確認」はできたが、「事前周知」が十分でないという課題は残る

■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

- 工場設備影響も含むセキュリティ事故発生時の**組織内連絡網の事前整備を確認**できた
- 参加者へ対応手順を示しつつ訓練を進めたことで、**対応手順の周知をより実施できた**

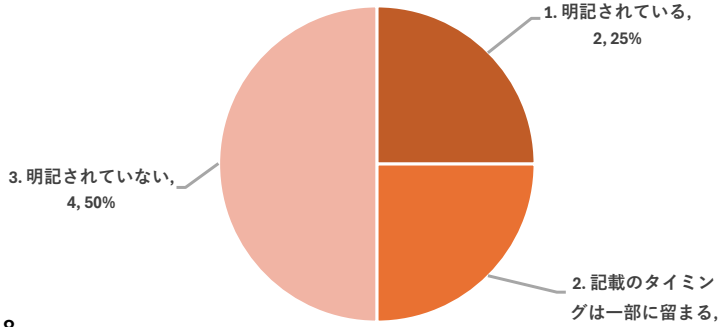
インシデント対応マニュアルが整備されつつある

インシデント対応マニュアルが整備されている。または、トラブル対応マニュアルが整備され、セキュリティ事故にも活用できる。



n=8
選択肢番号,選択肢,回答組織数,割合（%）

JPCERT/CCと連携するタイミングおよび内容について、インシデント対応マニュアル、またはトラブル対応マニュアルに明記されている。

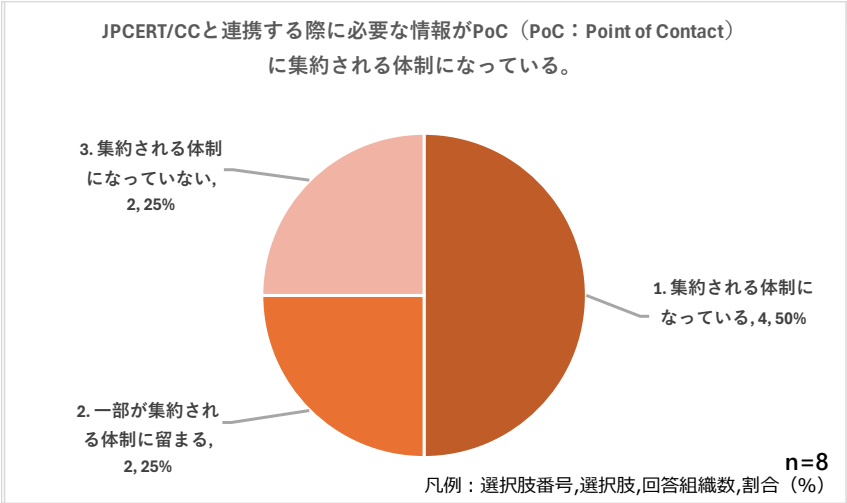


n=8
選択肢番号,選択肢,回答組織数,割合（%）

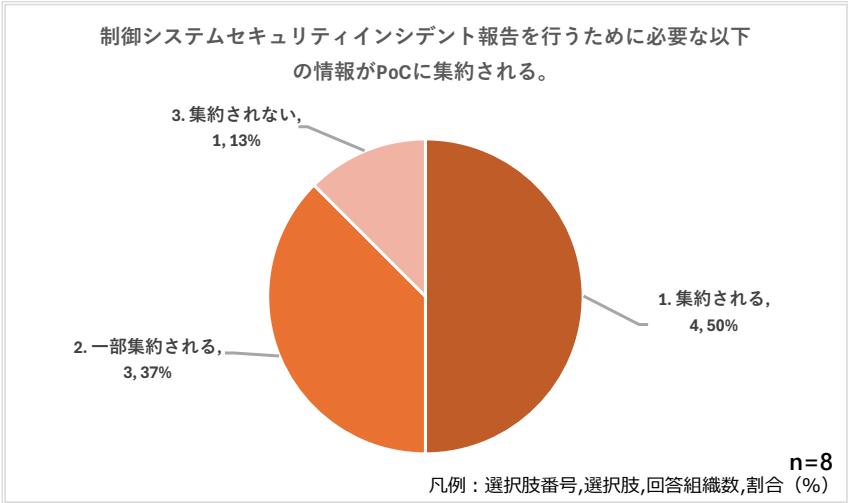
■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

- 工場設備影響も含むインシデント対応マニュアルの**事前整備を確認**できた
- インシデント対応マニュアルの**準備と活用が進みつつあることが確認できた（活用の途上）**

対外連携に必要な情報はPoCに集約される体制になっている



➢注
- PoC・・・Point of Contact（連絡窓口）を指す



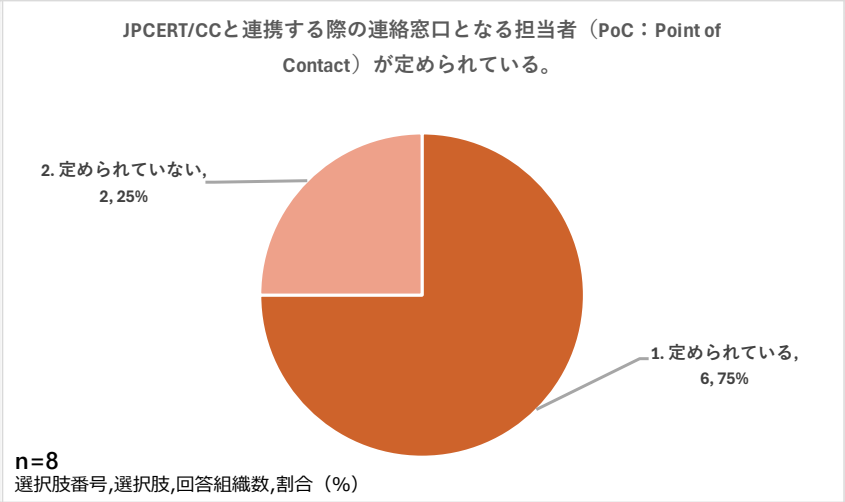
➢本設問の集約対象
- インシデントが発生した制御システムの情報
- 関連するOS・ソフトウェア・ハードウェアの情報
- 発生時刻、インシデントの内容、インシデントに関連するファイル

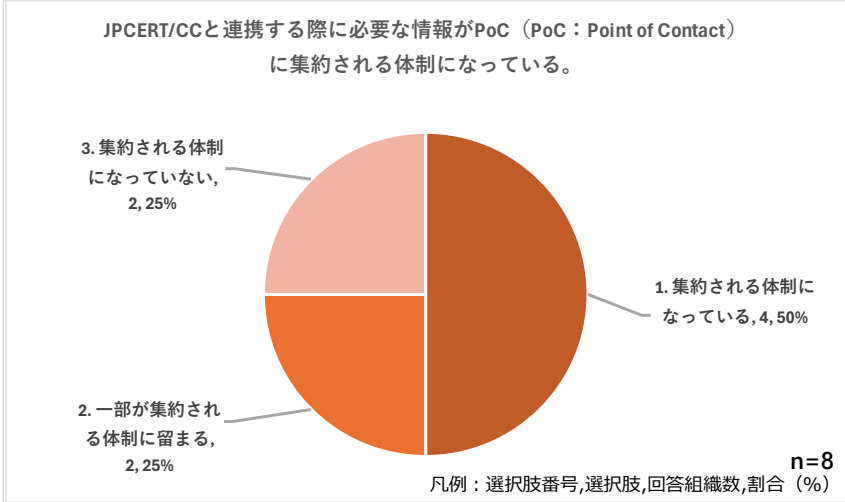
■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

➢ 組織内の情報集約体制が、**対外連携も視野に入れて整備が進みつつあることが確認**できた

➢ **集約すべき情報の理解も進みつつあることが確認できた（集約の途上）**

外部セキュリティ機関の連絡先の組織内周知が進みつつある





➢注
- PoC・・・Point of Contact（連絡窓口）を指す

■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

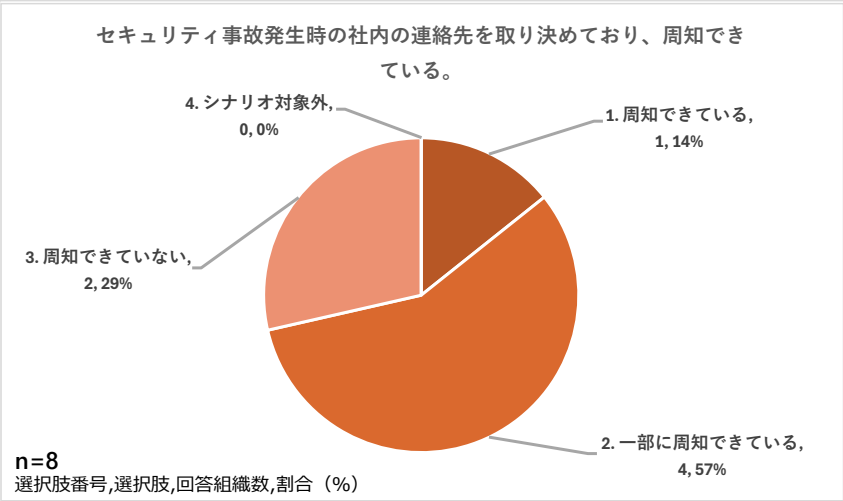
➢ 組織内体制整備における**対外連携機関の連絡先の周知が進みつつあることが確認**できた

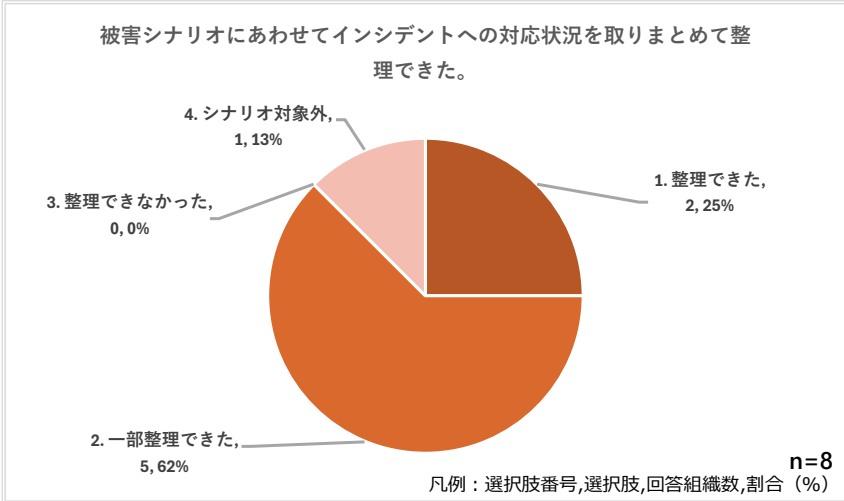
➢ **対外連携する際の担当者の明確化も進みつつあることが確認できた**

2. 俯瞰的な分析で見られた特徴（抜粋）

- b. 8社を俯瞰的に見た際に見られる特徴（課題点） -

組織内で連絡すべき内容の不明瞭さに課題

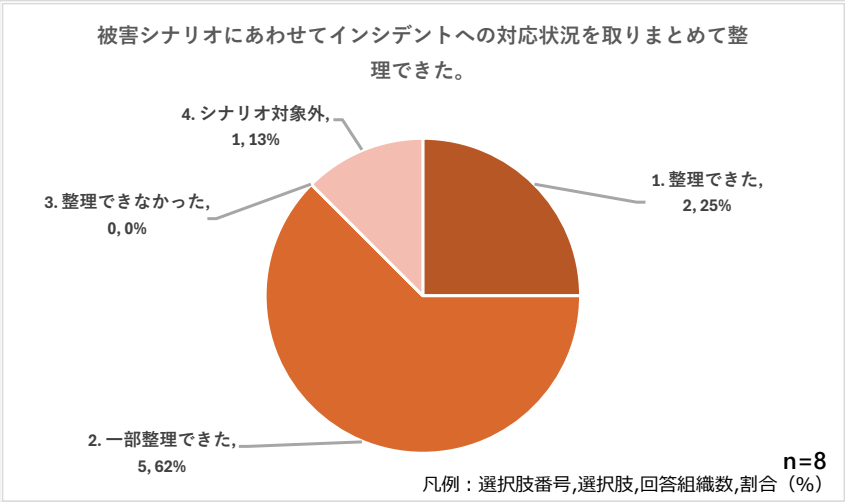


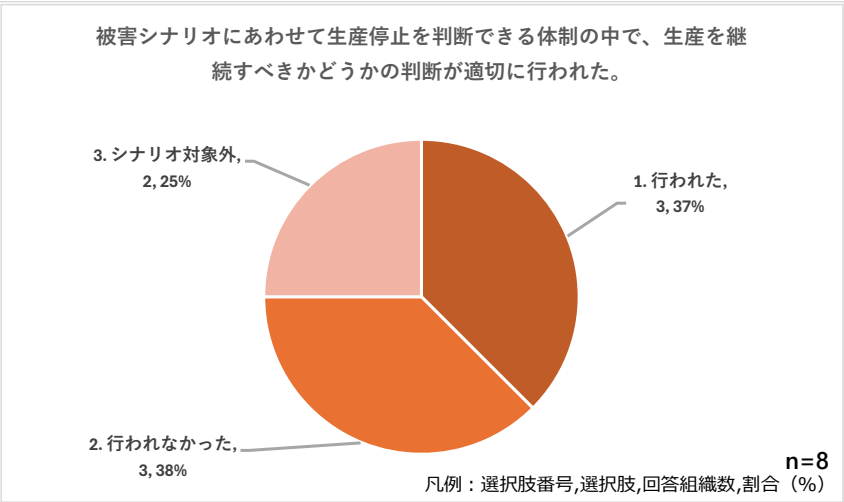


■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

- 組織内連絡網の事前整備は出来ているものの**「周知」が十分でないため連絡内容の考慮も同様**
- 状況整理が困難な一因に**「五月雨式な報告内容の精査時間」の不足と「整理手順」が不明確なこと**がある

対処のための情報の整理と活用に課題

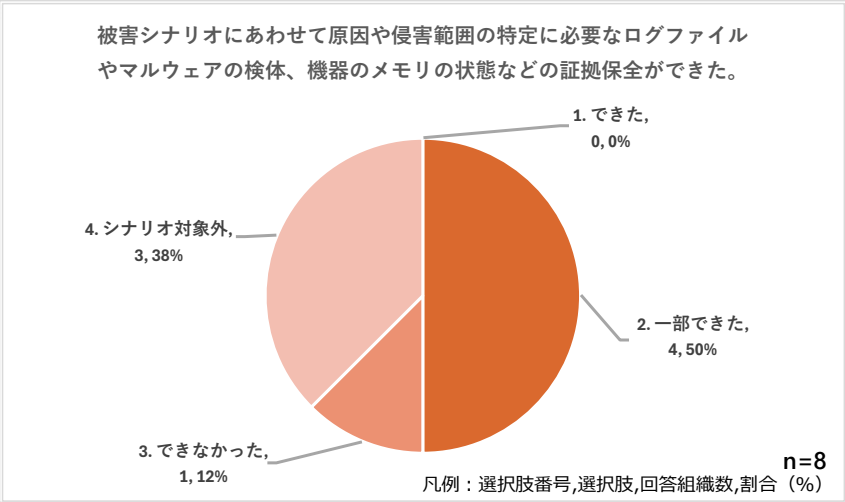


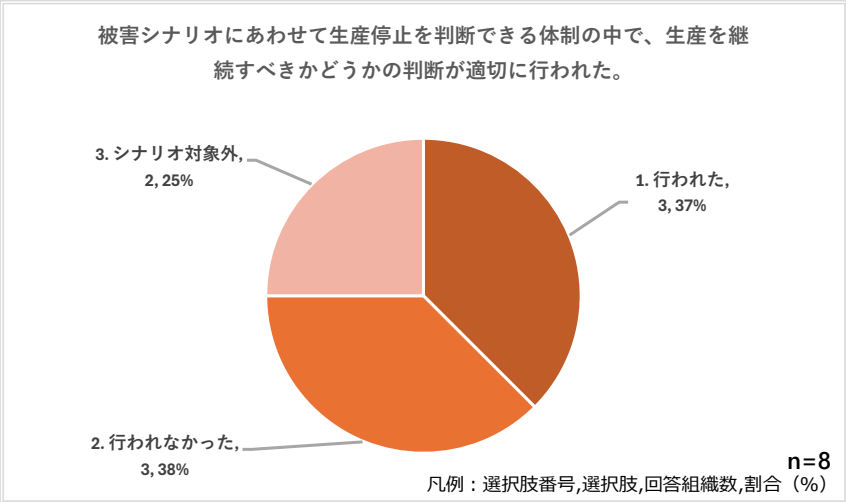


■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

- 一部整理できたものの**「整理」が進まなかったため「生産継続可否」の判断材料等の活用が進まず**
- 活用可能な情報があっても**「生産継続等の判断基準」が不明確で判断の「適切さ」に課題が残った**

証拠保全と事業継続の並行対応を見据えた事前準備に課題

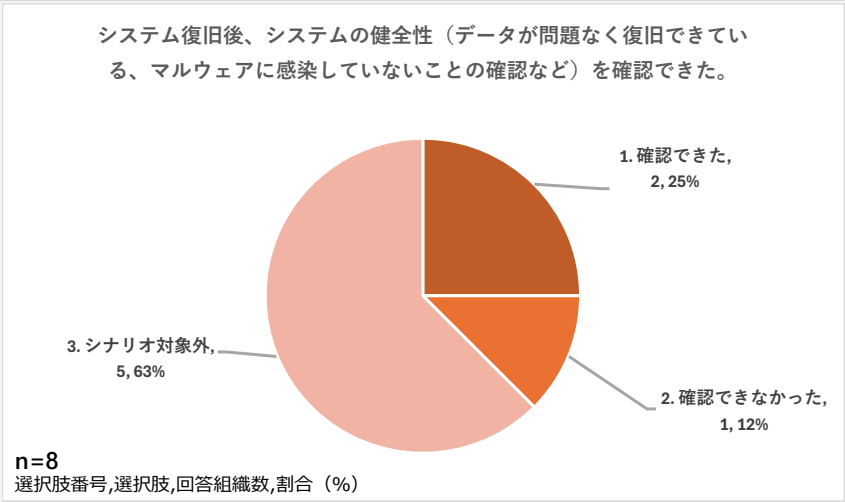


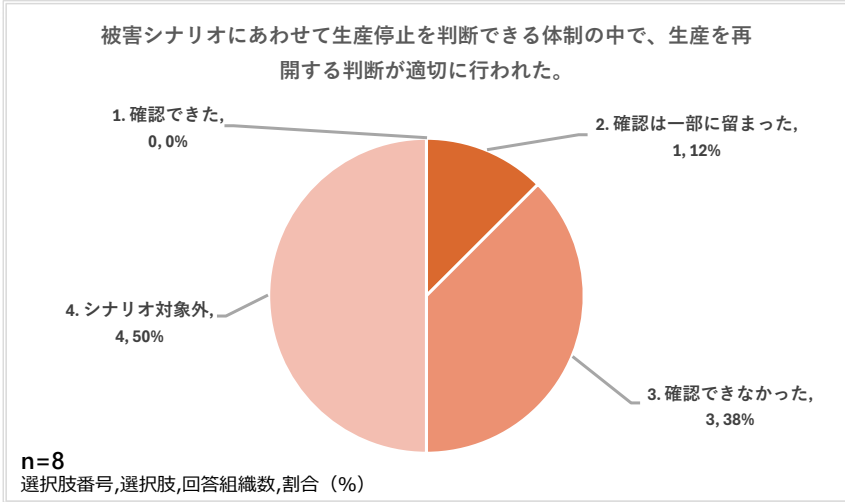


■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

- 保全が一部に留まる一因に**保全対象の範囲（設備や情報種別等）や保全手段が不明確なことがあった**
- 保全と平行した事業（生産）継続の対応が困難な一因に**「継続の判断基準の設定」「事前準備（対応優先度の設定やリソース確保）」があった**

生産を停止した場合の「再開判断」の決定要素の曖昧さに課題

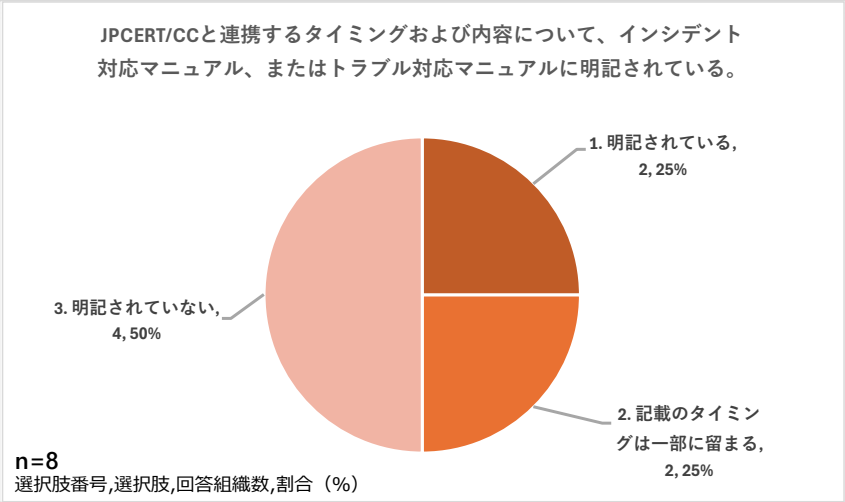


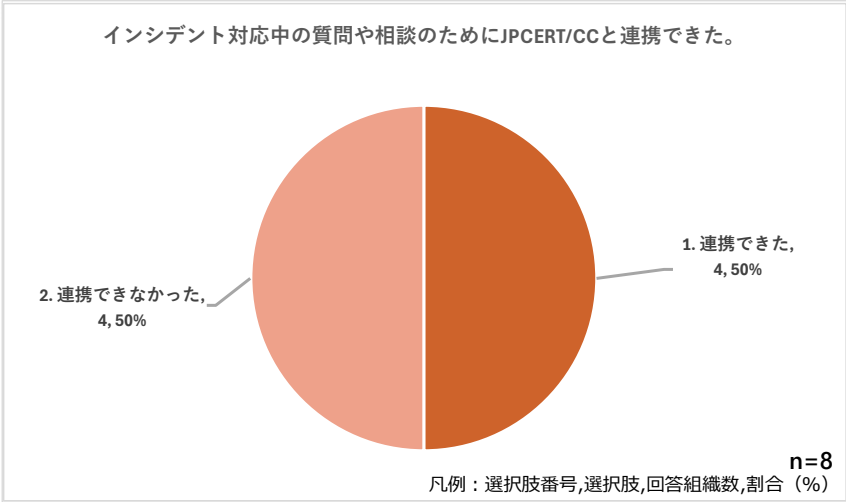


■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

- システムの健全性確認としてチェックツールによるマルウェア駆除完了確認を挙げるケースが多く、**より網羅性を担保する手段の確保ができていないという課題があった**（例：調査漏れ確認等の相談を外部セキュリティ機関へ行い自組織の視点だけでは気づけていない点を補う等）
- 生産再開判断ができなかった一因に**「再開判断基準の事前設定」がなく「判断材料となる情報の十分な収集」もできていないという課題があった**

訓練が組織内対応で完結しやすく外部連携の有効活用に課題





■ **これらの評価結果（提出された各組織の分析コメントを含む）から見える特徴**

- 有事の実対応時に外部連携の想定が少ないためか**「訓練」での対外連携確認が少ないことが分かった**
- 対外連携への理解が浅いためか**「対外連携の対応フロー」の整備が十分でないということが分かった**

3. トークセッション

- 見られた特徴や課題等をさらに深掘り -

まとめ：トークセッションの前に

- **これらの特徴から言えること**

「訓練」の意義や価値をより踏まえた工夫や意識が伺える

インシデント対応の準備は途上であり「体制の成熟」に期待

対外連携は十分に活用できておらず「連携対処」視点が今後の重要な課題

「訓練」とは何か？を踏まえて日ごろから備え、
「連携対処」する関係の構築が期待される

トークセッションでさらに深掘り ⟶

各種お問い合せ、ご相談は

情報収集やセキュリティ評価など、IT／OTセキュリティで困ったら、
下記へお気軽にお問い合わせください。

■ **情報系・制御系セキュリティに関する各種ご相談・調査依頼等**
国内コーディネーショングループ

— Email：dc-info@jpcert.or.jp

— https://www.jpcert.or.jp/ics/

■ **制御システムのインシデントに関する報告やご相談**
インシデントレスポンスグループ

— Email：info@jpcert.or.jp

— https://www.jpcert.or.jp/ics/ics-form.html

※資料に記載の社名、製品名は各社の商標または登録商標です。

Thank you!