工場が昔からやっていた「備え」に学ぶ、制御システムインシデント対応

2026年2月10日(火) 制御システムセキュリティカンファレンス2026

Claroty Ltd. APJ Sales

Senior Solution Engineer 加藤　俊介

発表者紹介

プラント出身のセキュリティエンジニア！
FS Eng (TÜV Rheinland, #19213/19, Safety Instrumented System)

加藤 俊介(Shunsuke Kato)

日系化学メーカにてキャリアを開始し、計装・制御システムエンジニアとして新設プラントの立ち上げや既設プラントのDCS更新プロジェクト、設備増強プロジェクト、海外プラントにおけるコミッショニング(立ち上げ・試運転)などに従事。
その後、制御機器メーカにて石油、化学向けの安全計装システム（SIS）の導入やサイバーセキュリティアセスメントを行う。現在はクラロティにて日本の製造現場を「より安全に、よりセキュアに」すべく日々邁進中。

JPCERT/CC: 制御システムセキュリティカンファレンス2023, 2024, 2025 登壇

Mission：「セーフティ x セキュリティで安心・安全な製造現場の実現！」

<現在>
- クラロティ 営業部　シニアソリューションエンジニア 2022年5月～
- JNSA 調査研究部会 OTセキュリティWG SWG-3 リーダー 2024年8月～

<これまでの経歴>
- 外資系 エナジーマネジメント & ICSベンダー企業 (4年)
  安全計装システム(SIS/TMC) エンジニア、OTセキュリティビジネス開発

- 日系化学メーカー (3年)
  計装・制御システム(DCS, PLC)エンジニア

NCEES　TÜVRheinland　ISA/IEC 62443 CYBERSECURITY EXPERT ISA

CLAROTY

OTセキュリティ関連インシデントの振り返り

2024 Threat Report - Cyber Incidents With Physical Impactより

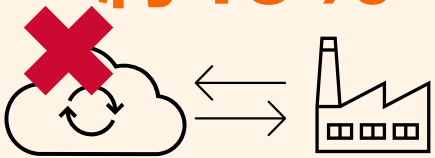
← 合計 約80%：IT起因による「間接的」なOT停止 →
(OTそのものは攻撃されていない)

約40%

念のための停止

OTは無事だが、被害拡大防止や安全確認のため、組織が自らの判断で停止。
ポイント：攻撃者の位置が不明な段階での「安全側への判断」。

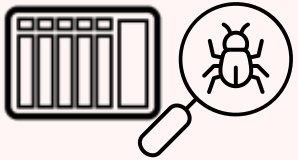
約40%



依存関係による停止

OTは稼働可能だが、依存するIT側システム（出荷・課金等）がダウンし、ビジネスプロセスが継続不可に。

約20%



直接的なOTへの影響

攻撃者がOTネットワークに侵入し、制御システムを直接的に暗号化、破壊、操作。
IT/OT分離の不備による感染拡大が主な原因。

https://www.youtube.com/watch?v=l4KduoIWVCg

CLAROTY

テーマ選定の背景

「直接的なOTへの影響」においては、サイバーインシデントという枠組みに囚われず、工場で培われてきたインシデント対応、安全設計の考えが応用できるのでは?

約20%

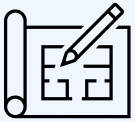
直接的なOTへの影響

攻撃者がOTネットワークに侵入し、制御システムを直接的に暗号化、破壊、操作。
IT/OT分離の不備による感染拡大が主な原因。

工場の「備え」を整理して、これまでのインシデント対応事例と照らし合わせることで、新たな知見・気づきを得られると仮説し、テーマ選定

インシデントに対する工場における「備え」

【設計】本質的安全設計



リスクを根源から断つ「持たない」設計

- 最小化・代替：危険物量やエネルギーの削減、安全な物質への転換。
- 緩和：低温・低圧運転によるプロセスの安定化。
- 簡略化：エラーを誘発しないシンプルな配管・操作系の構築。

【実装】高度な信頼性と防護

故障や攻撃を前提とした「耐える」技術

- 高信頼ロジック：2oo3（冗長化）による可用性と安全の両立。
- ゼロリカバリ通信：PRP/HSRによる通信途絶ゼロのネットワーク。
- 物理防護：フェイルセーフ設計（NC設計）

【運用】知能化保全と適応力

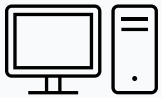
異常を「予見」し、迅速に「回復」する力

- 予兆保全：AI・データ分析による故障早期検知。
- 意思決定支援：アラーム合理化とデジタルSOPによる現場判断の迅速化。
- 自律的回復：インシデント発生時の自律的な機能維持と復旧プロセスの確立。

【共通基盤（レジリエンスの土台）】

「多層防御（LOPA）」によるリスク低減の最大化

設計（ISD）



基本制御（BPCS）

警報・介入

安全計装システム（SIS）

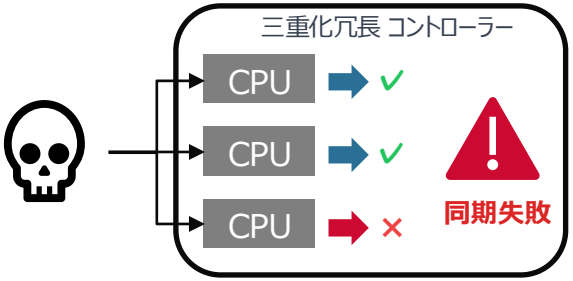
物理的防護

非常時対応

TRITON攻撃失敗の真相：『三重化冗長』の勝利

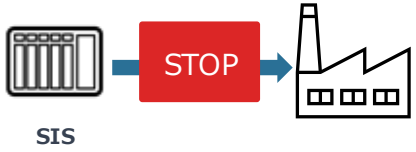
システムの安全設計による防御がサイバー攻撃に対して成功した例

1. 攻撃コード実行と同期失敗



3つのプロセッサ間で処理結果に
不一致が発生。

2. フェイルセーフ(安全側への停止)の作動



システムは不整合を『危険な故障』と
みなし、自動的にプロセスを安全停止。

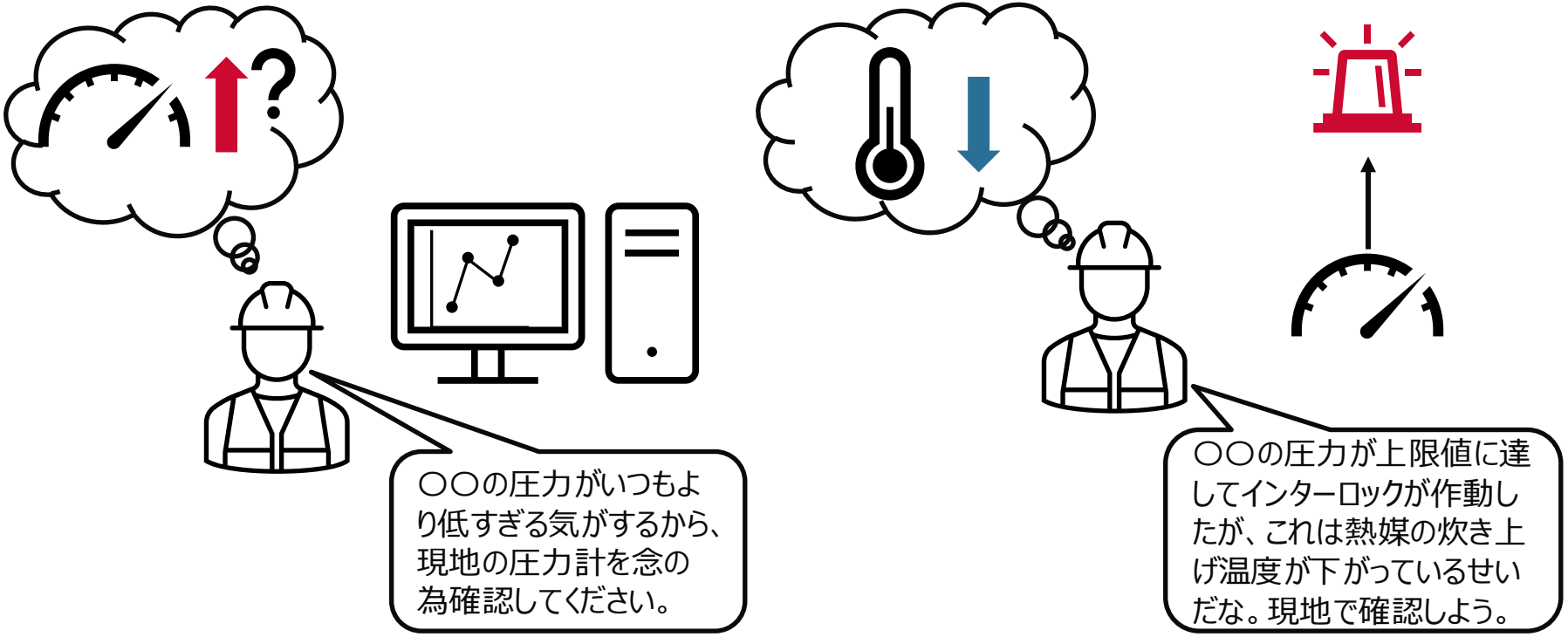
3. インシデント発覚とマルウェア発見

詳細なフォレンジック
調査でTRITONを発見。

論理的な侵入は許したが、システムの堅牢な安全設計（冗長性）が最終的な破壊を阻止した。

インシデントへの工場における「備え」-知能化保全と適応力

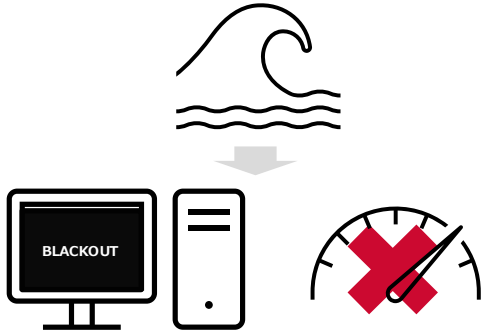
現場の物理法則に対する少しの違和感や、要因の結合性を理解している。



福島第一原発事故の事例

デジタル消失時の物理的実体による生産活動維持の具体例

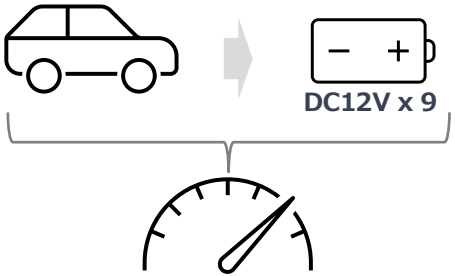
1. 津波による電源喪失



津波により非常用電源を含む電源喪失。計測機器の電源もブラックアウトし、**監視不能状態**に。

https://www.nrc.gov/docs/ml1134/ml11347a454.pdf

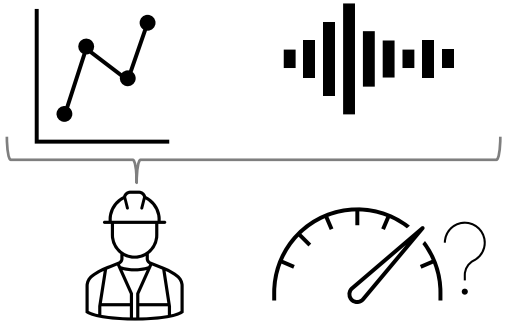
2. バッテリー集めと計器復旧



事業所内の車から**バッテリーを回収し、配線作業を手作業**で実施したうえで、計測機器を復旧。

https://www.nrc.gov/docs/ml1134/ml11347a454.pdf

3. 誤表示とクロスチェックによる特定



基準液面の蒸発により、水位計は誤表示。爆発音や線量上昇などの**物理現象から誤表示**を断定。

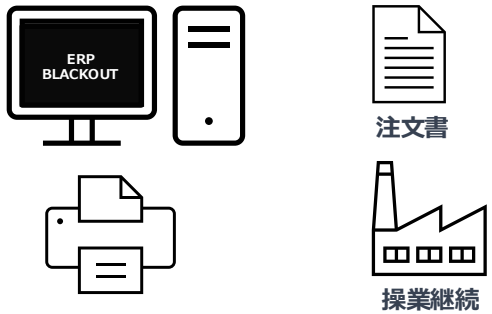
https://rief-jp.org/ct10/8601

デジタルと切り離された物理層で直接対象に介入する能力と手段は最後の防衛線である。

ノルスク・ハイドロの事例

デジタル消失時の物理的実体による生産活動維持の具体例

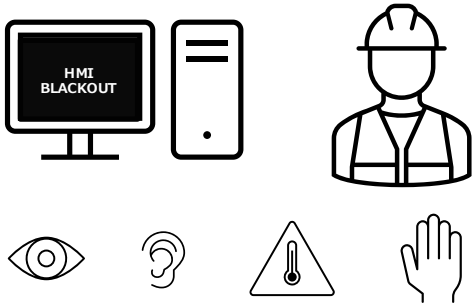
1. 紙のバックアップ（ベルギー工場）



ERPダウンでも、毎週印刷していた「リングバインダー」の紙資料で操業継続。「リヒターフェルデの英雄」。

https://www.havtil.no/en/explore-technical-subjects2/technical-competence/features/2023/ransomware-taught-key-lessons/

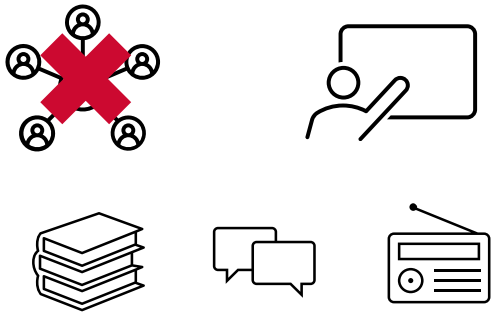
2. 五感と物理介入（製錬炉）



HMI停止時、ベテランが「色・音・熱」で状態判断。手動操作で凍結を防ぎ、設備全損を回避。

https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

3. アナログ事務と通信（運用管理）



通信途絶時、倉庫の「紙マニュアル」や「ホワイトボード」で情報共有。スマホやトランシーバーも活用。

https://www.hydro.com/en/global/about-hydro/stories-by-hydro/employees-find-creative-solutions-in-response-to-cyber-attack/

デジタルが消失しても、「物理的な実体（紙の記録、人間の五感、物理的な操作）」によってビジネスの核となるプロセスを維持できる代替手段の確保が重要。

OTセキュリティ関連インシデントの振り返り(再掲)

2024 Threat Report - Cyber Incidents With Physical Impactより

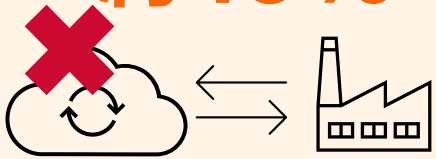
← 合計 約80%：IT起因による「間接的」なOT停止 →
(OTそのものは攻撃されていない)

約40%

念のための停止

OTは無事だが、被害拡大防止や安全確認のため、組織が自らの判断で停止。
ポイント：攻撃者の位置が不明な段階での「安全側への判断」。

約40%



依存関係による停止

OTは稼働可能だが、依存するIT側システム（出荷・課金等）がダウンし、ビジネスプロセスが継続不可に。

約20%

直接的なOTへの影響

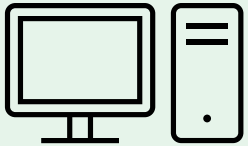
攻撃者がOTネットワークに侵入し、制御システムを直接的に暗号化、破壊、操作。
IT/OT分離の不備による感染拡大が主な原因。

依存関係にあったIT側システムをアナログな手法で運用し、操業を継続させることも可能。

依存関係による停止：制御システムが無事でも事業は停止

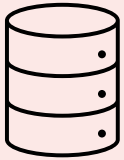
制御システムは無事であっても、密結合した上位システムの停止が結果的に操業影響を及ぼす。

Colonial Pipeline事件



パイプライン制御システム

✓ **無事・稼働可能**



計測・請求システム

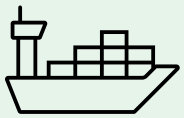
× **ダウン・使用不能**

「誰に・どれだけ」の情報を喪失

操業を停止

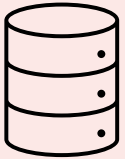
請求プロセスが機能せず、
ビジネスとして継続不可能に。

Maersk（海運）NotPetya事件



船やクレーンの制御システム

✓ **無事・稼働可能**



コンテナ追跡システム

× **ダウン・使用不能**

「どこへ運ぶか」の情報を喪失

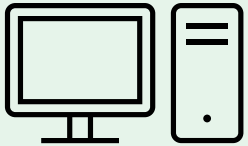
物流が停止

行き先が不明となり、
荷役作業が完全にストップ。

依存関係による停止：機能縮退対応により操業継続

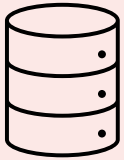
密結合した上位システムを機能縮退したオペレーションによって操業を継続

アサヒGHDにおけるランサムウェア攻撃



工場の制御システム

✓ 無事・稼働可能



受発注・出荷システム

× ダウン・使用不能

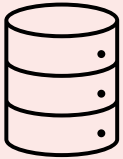
受発注システム

△ 電話/FAXによる手動対応

大阪急性期・総合医療センターにおけるランサムウェア攻撃

医療機器オペレーション

✓ 無事・稼働可能



医療ITシステム

× ダウン・使用不能

医療システム

△ 紙カルテによる手動対応

機能縮退時のオペレーション検討

アナログからITへの変遷と、非常時の備えとしての『アナログの再評価』

アナログ機器によるオペレーション(過去)

電子化・IT化

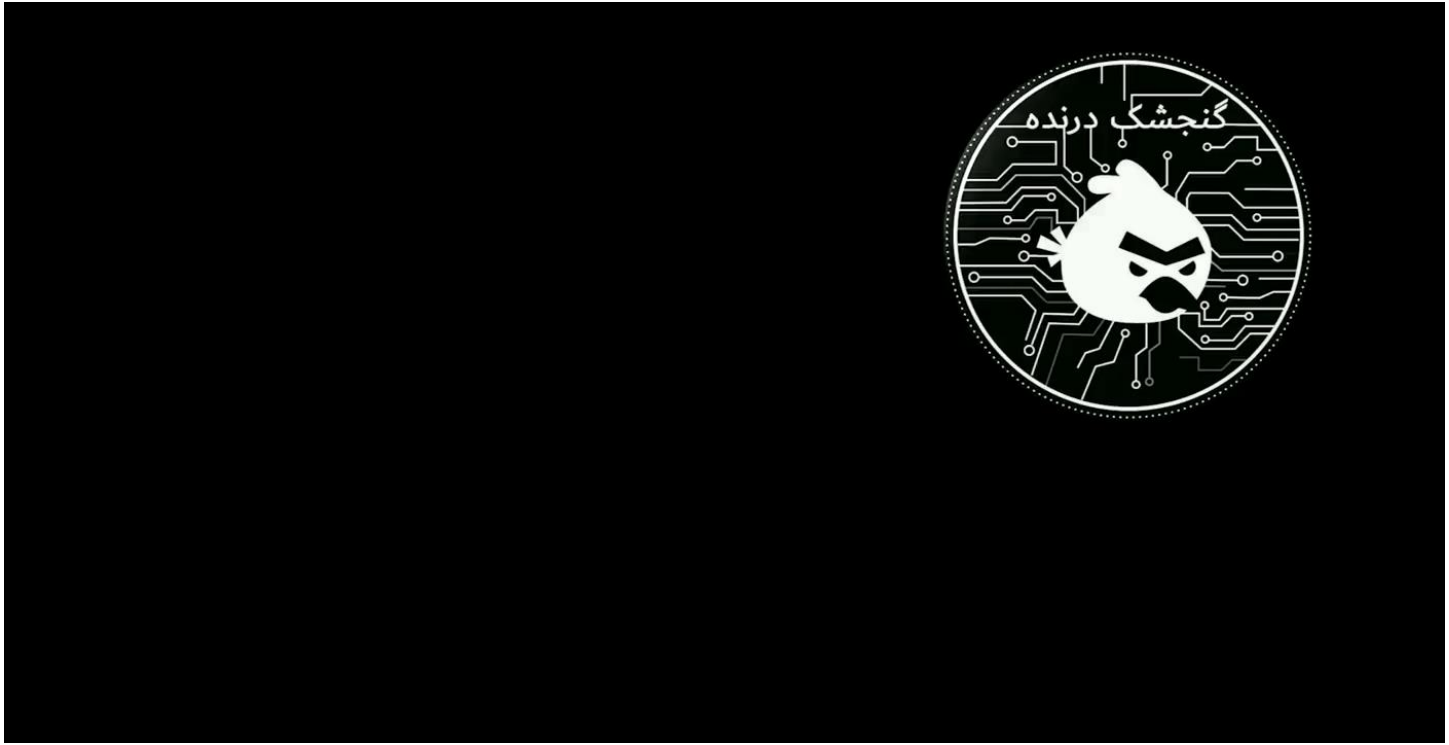
有事の機能縮退

IT機器によるオペレーション(現在)

IT化されたシステムについては常に停止するリスクと隣合わせであり、その際の対応策としての”オペレーショナル・テクノロジー(運用・技術)”を改めて文書化、プロセス化して定着させる必要がある。

サイバーインシデント=>設備破壊事例

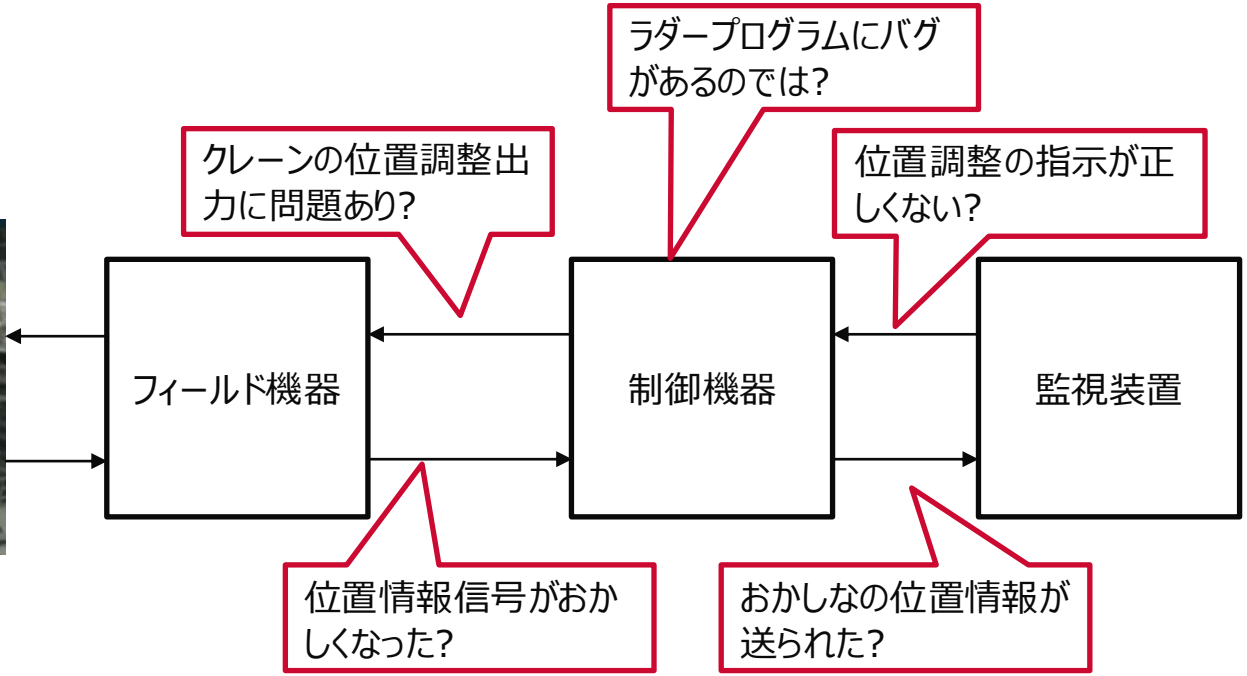
@GonjeshkeDarand



https://x.com/GonjeshkeDarand/status/1541288345183158272

インシデント調査のポイント (計装エンジニア視点)

制御対象



インシデント調査 (計装+セキュリティエンジニア視点)

制御対象

脆弱性を突かれて、
RCEでプログラム変更?

ラダープログラムにバグ
があるのでは?

マルウェアによる不正
操作指示がされた?

クレーンの位置調整出
力に問題あり?

位置調整の指示が正
しくない?

フィールド機器

制御機器

監視装置

位置情報信号がおか
しくなった?

おかしなの位置情報が
送られた?

入力信号が
書き換え?

フィジカル空間 x サイバー空間、両面でのインシデント調査が必要になる。

個社レベルを超えたインシデント対応(共助・公助)

有事における「競争の超越」：産業事故から学ぶ究極の復旧作

アイシン精機（1997年）

トヨタ車両向けブレーキ部品（Pバルブ）**主力工場が全焼失**。ジャスト・イン・タイム（JIT）で在庫極少、数日以内に**国内全ライン停止の危機。**

民間連携

競合メーカー含む200社以上が協力。特許・**ノウハウ含む詳細図面を直ちに他社へ公開。**競合他社や異業種が金型を急造して代替生産、わずか**5日で部品供給再開。**

https://www.sydrose.com/case100/shippai-data/315/

信越化学工業（2007年）

メチルセルロース製造部門で**爆発火災。**医薬品添加剤の供給停止。国内ほぼ100%シェアで代替品なく**医療現場への深刻な影響懸念。**

行政介入

厚生労働省が「緊急措置」発動。詳細スペック(**事実上の秘匿レシピ)を他社・製薬企業へ公開要請**、同社も応諾。代替品切り替えの法的手続き（承認申請）を事後対応**で許可、代替生産を加速。**

https://www.wam.go.jp/wamappl/bb11gs20.nsf/0/59bf465d928b3b9b492572c7002dccc5/$FILE/20070424_6shiryou.pdf

ルネサスエレクトロニクス（2021年）

主力**工場の火災**により、世界的に不足していた車載半導体の**供給がさらに逼迫。**

官民一体

顧客企業と国が支援。トヨタ・日産などが**技術者派遣で支援。**経済産業省が外交・行政ルートで代替装置を最優先納入。海外ファウンドリ(TSMC等)による**代替生産も実施。**

https://toyokeizai.net/articles/-/426165?display=b

火災ではなくランサムウェア感染による事案の発生リスクも今後は考慮が必要。

もし計装エンジニアに戻ったら：現場アクション・チェックリスト

現場チェックリスト: サイバーインシデントに備えるための具体的な確認事項

HMI/ENGSの予備所在確認と復旧訓練

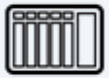
最低限の予備品が事業所内にあるか？

実際にバックアップから復旧できるか練習したか？

UPSのネットワーク接続確認（マルウェア対策）

UPSがネットワークに接続されていないか?

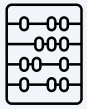
デジタル経由の攻撃を受けない?



制御コントローラー予備品の確認

予備として保管されているか？

他事業所には保管されているか?



インターロックの物理的独立性確認

デジタルから切り離して安全にシャットダウンできる?

サイバー攻撃の影響を受けずに止められるか？

運転員との『もしも』の机上訓練

どのようなアナログ運転が可能？

最低限どのプロセス値を監視すべき?

P&IDを用いた手動監視・操作ポイントの特定

手動で監視・操作できるポイント確認したか？

図面と現地でのそのポイントの整合性は合ってるか?

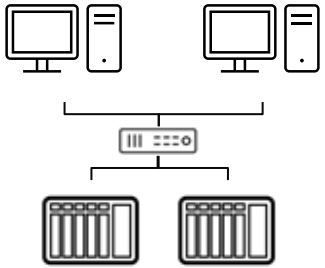
サイバーセキュリティの知見がなくても、出来ることはある。

インシデントからの安全な復旧：再稼働判断のための3基準

Lessons Learned From the Front Lines of OT incident Responseより

基盤（Foundation）

MVA:Minimum Viable Architecture
最小実行可能なアーキテクチャ



操業再開に最低限必要なインフラ、資産、情報。
デジタル資産だけでなく、P&ID等の図面・文書類も必須（法的要件）。

事業（Business）

MVP：Minumum Viable Process
最小実行可能なプロセス

ビジネス継続に最低限必要な物理的な生産・制御プロセス。
全てではなく、「稼ぐための最重要設備・ライン」にリソースを集中。

防御（Defense）

MVC：Minimum Viable Controls
最小実行可能な統制

MVAとMVPを維持・保護するための最低限のセキュリティ・安全管理策。
再攻撃を防ぎ、環境に対する確実な制御権（ポジティブコントロール）を維持。

https://www.youtube.com/watch?v=luWLgQZngxI

3要素の確保＋BCPとの整合性を取ることで再稼働宣言できる状態を準備する。

CLAROTY

有事における生産継続の意思決定マトリクス

操業継続するための判断基準とルート選択

Phase 1：インシデント検知・初動

RANSOMWARE DETECTED

トリガー：

ランサムウェア等によるシステム機能不全の発生。

「制御・通信が奪われた状態で、物理的な生産手段は生きているか？」

Phase 2：継続ルートの選択

ルートA
【アナログ・マニュアル継続】（最速・暫定）

判断基準: デジタル要素を切り離した「手動・単独運転」が可能か？
アクション: アナログ計測器、手動バイパス、現場操作への切り替え。

ルートB
【デジタル予備からの復旧】（中長期・安定）

判断基準: 汚染されていないデジタル資産はあるか？
アクション: スペアパーツへの交換、バックアップからの再構築。

ルートC
【外部・代替リソース活用】（組織的補完）

判断基準: 自拠点での継続が不可、または復旧に時間を要するか？
アクション: 在庫の放出、他拠点での増産シフト、生産委託。

Phase 3：時間軸とインパクトの評価

要求時間（RTO）：

暫定運転でいつまで持ちこたえる必要があるか？

許容停止時間：

事業への致命的な打撃を避けるための「限界」はどこか？

Phase 4：最適プロセスの策定

成果物：

選択したルートに基づいた「緊急時運転プロセス」の即時適用。

CLAROTY

まとめ

1. 制御システムは元来求められてきたミッションクリティカルな運転要求から、万が一の事態への備えが現場知識として養われている。万が一の**事態は必ずしもサイバー要因ではない。**

2. サイバーインシデント発生時には、”機能縮退”した上での運転継続が求められる。”機能縮退”時にどのような**最低限の備えがあれば運転を継続**できるかは、プロセス設計、製造課部門などとのの議論が必要。

3. 機能縮退したアナログによる暫定復旧、デジタル予備による復旧、外部・代替リソース活用など**組織としての選択肢を確認**しておくことで、有事に備えられる。

制御システムのインシデント対応強化には、より一層**”OT(運用・技術)”**を深く知ることが重要である。