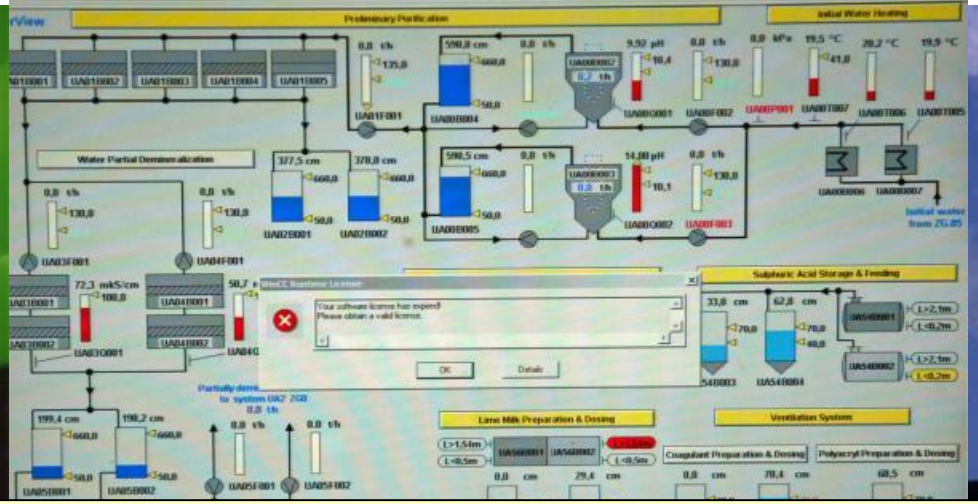
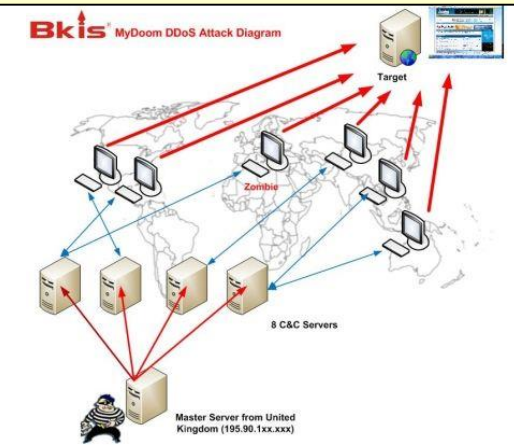


# 2020年に実施した新型コロナ対策アンケート結果の紹介とリモートが進んだ状況下でのサイバーセキュリティについて


**橋本芳宏（名古屋工業大学）**

http://www.manage.nitech.ac.jp/Security


**化学工学会SIS部会**
**プラントオペレーション分科会**
**「WithコロナAfterコロナを捉えたプラントオペレーションを考える」**
2022年3月22日（オンライン）

# 自己紹介　橋本芳宏 1957年12月1日（生）64歳

名古屋工業大学 社会工学科 経営システム分野 教授

http://www.manage.nitech.ac.jp/Security

（制御系セキュリティに関して）

2011年～2012年　経済産業省

　制御システムセキュリティ検討タスクフォース人材育成WG 委員

2012年～2014年　IPA（情報処理推進機構）

　制御システムワーキンググループ委員

2016年～2019年　内閣府 戦略的イノベーション創造プログラム

　重要インフラ等におけるサイバーセキュリティの確保

　セキュリティ人材育成 委員

2017年～　IPA産業サイバーセキュリティセンター講師

　　名古屋工業大学の研究室でのサイバー攻撃のデモには

　　2013年以来、のべ600名以上来訪

（プロセス制御に関して）

2010年～　計測自動制御学会 プロセス塾講師

2008年～2017年　化学工学会プラントオペレーション分科会副代表

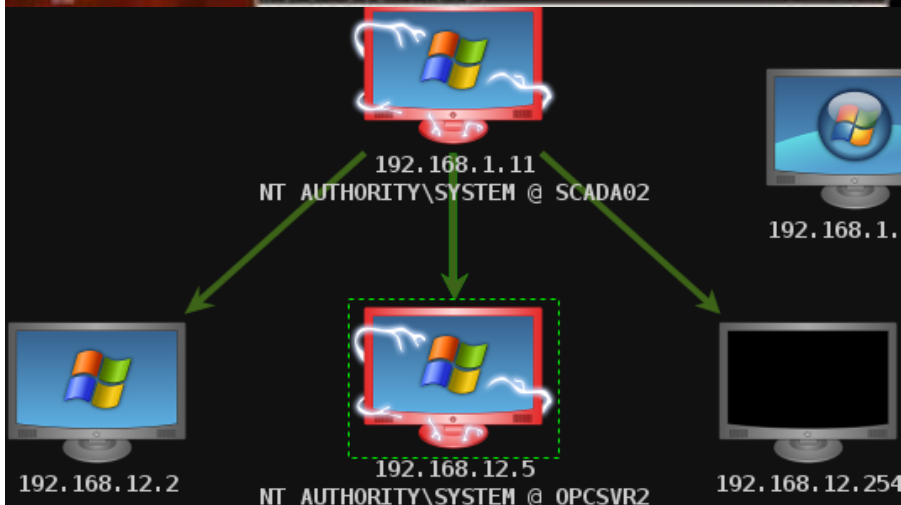
（略歴）

1985年　京都大学大学院化学工学専攻博士課程（単位取得退学）

1985年　名古屋工業大学 生産システム工学科 助手

2003年　名古屋工業大学 システムマネジメント学科 教授

　　学内組織再編を経て、現在にいたる



# 本日の話題

## 【第1部】

- **新型コロナウィルス禍における操業現場の対応に関するアンケート調査**

  2020年11～12月実施結果の紹介

- セキュリティ対策はできているとの回答が多いが本当に大丈夫？

## 【第2部】

**リモートが進んだ状況下でのサイバーセキュリティ**

- サイバーセキュリティのあるべき姿とは？
  - どれだけやっても十分になることはない！
  - **これだけやっておけばよいというレベルが示されることもない。**
- セキュリティへの投資をさぼると、どんなリスクが？
- **セキュリティで信頼できる企業と評価されるためには？**

**NIST CSF（Cyber Security Framwork）**



みんながわかる言葉で課題共有

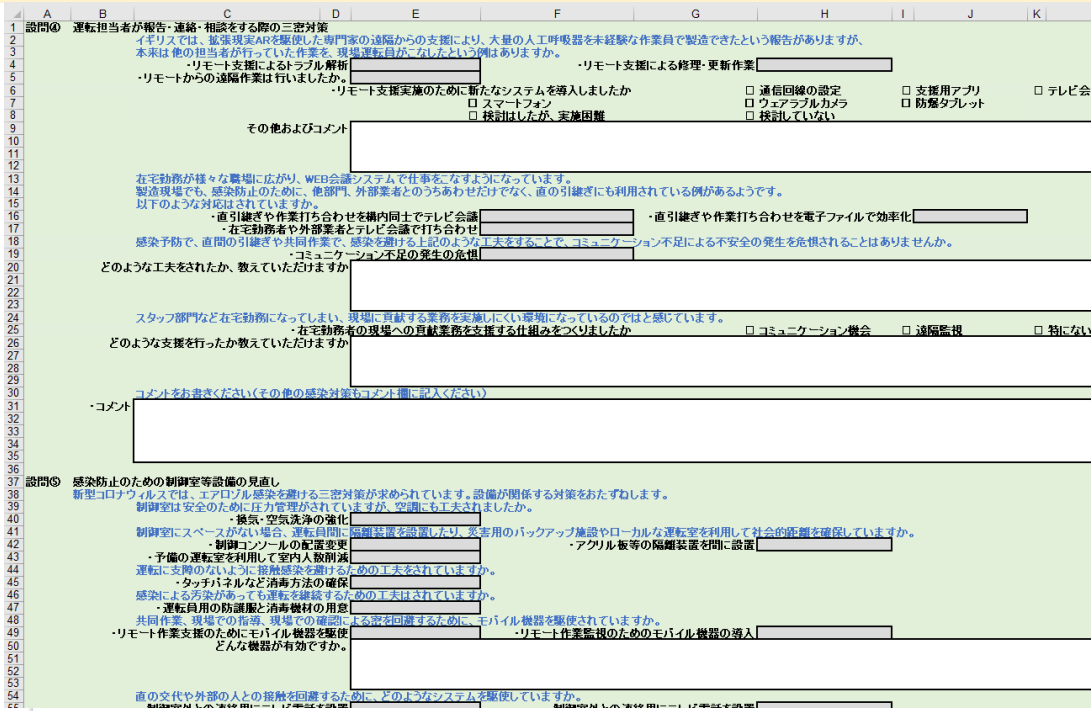
# 【第1部】

# 新型コロナウィルス禍における
# 操業現場の対応に関するアンケート調査
# 2020年11～12月実施結果の紹介

# 新型コロナウィルス禍における操業現場の対応に関するアンケート調査


## COVID-19操業現場対応アンケート合同調査委員会

SICE 安全のための計測・制御・システムを考える会
化学工学会SIS部会 プラントオペレーション分科会
JEITA 制御・エネルギー管理専門委員会 WG3



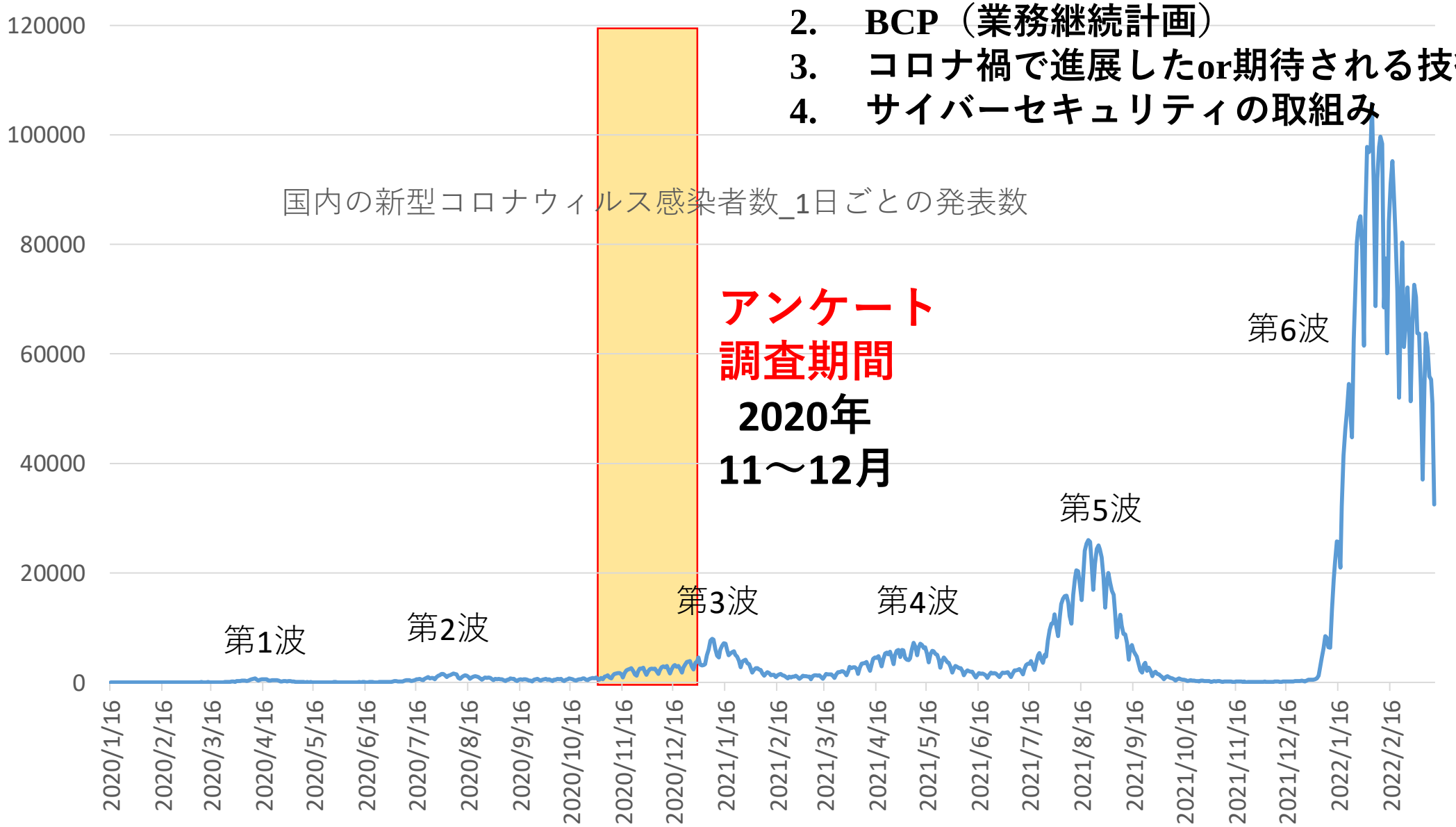

https://www.sice.jp/info/info_press/press_20210623.html

# アンケート調査

コロナ禍をきっかけに、オフィスはリモートワークで大きく変わったが、操業現場の変化は？

設問 大項目14 （回答欄）283の大規模アンケート

1. **パンデミックから操業を守る感染症対策**
2. **BCP（業務継続計画）**
3. **コロナ禍で進展したor期待される技術**
4. **サイバーセキュリティの取組み**



# 回答者（全45事業所）

回答者の業種・職種
- 化学、石油、ガスで7割以上
- 工場管理部門で2/3

回答者のCOVID-19 への意識
- 7割が長期化すると予想

COVID-19対策生活様式が不要になる時期予想
- 多くが2，3年後とする中、1割は今後ずっとと予想

ワクチンや治療法が確立し，
風邪やインフルエンザと同等になる時期予想
- 8割が2,3年かかると予想

このアンケートに対する関心
- 他社の取組みを知りたいという回答が多い

⇓

2021年3月に回答者に集計結果報告
2021年6月にSICE WEBで報告書を公開

新型コロナウィルス禍における操業現場の対応に関するアンケート報告書

ttps://www.sice.jp/info/info_press/press_20210623.html　123頁

# 操業現場の変化

- プラント停止

| 選択肢 | 中長期の停止 | 短期の停止 | コロナ禍での停止はない | 無回答 | 合計 |
|---|---|---|---|---|---|
| 回答数 | 1 | 3 | 35 | 6 | 45 |

**サプライチェーンの破綻や需要低下による停止がわずかにみられた**

**七尾鉄道やJR函館線のような社員の感染による操業停止はみられない**

- 生産量・稼働率の低下

| 選択肢 | 中長期の低下 | 短期の低下 | 操業状態の変化なし | 無回答 | 合計 |
|---|---|---|---|---|---|
| 回答数 | 7 | 21 | 15 | 2 | 45 |

| | 中長期的要因 | 短期的要因 | 無回答 | 合計 |
|---|---|---|---|---|
| 運転員の感染あるいは感染予防 | 5 | 9 | 31 | 45 |
| 需要の衰退 | 9 | 22 | 14 | 45 |
| サプライチェーンの破綻 | 3 | 13 | 29 | 45 |

**生産量・稼働率の低下は6割以上で発生**

**感染対策を低下の原因にあげている回答は14件で28件の半数におよぶ**

**感染者が発生した時の対応が難しくなるので、年末年始の稼働を取りやめたという回答もあった。**

# 運転体制の変化

| | 中長期的にも適用 | 短期での実施 | 検討したが実施してい | 検討していない | 無回答 | 合計 |
|---|---|---|---|---|---|---|
| 出勤者を減らすための運転体制の変更 | 4 | 5 | 15 | 13 | 8 | 45 |

**2割は変更を実施、6割が検討している。**働き方改革の一環として実施した例も
プラントの優先順位を決めて、人員計画を策定した例も

| | 中長期的にも適用 | 短期での実施 | 検討したが実施してい | 検討していない | 無回答 | 合計 |
|---|---|---|---|---|---|---|
| 昼勤の一部在宅化 | 7 | 9 | 9 | 15 | 5 | 45 |
| 直の一部在宅化 | 2 | 1 | 6 | 30 | 6 | 45 |
| 直の在宅化の新たな業務設定 | 1 | 1 | 5 | 28 | 10 | 45 |

**昼勤には在宅の導入例はあるが、4割弱である。**
**直の在宅化は、ほとんどない。**事故時の対応を考慮すると困難との回答
**直を在宅化している例では、新たな業務を設定**

| | 中長期的にも適用 | 短期での実施 | 検討したが実施してい | 検討していない | 無回答 | 合計 |
|---|---|---|---|---|---|---|
| 退職者や経験者による直編成 | 5 | 7 | 14 | 16 | 3 | 45 |
| 他のプラントへの支援参加教育 | 1 | 3 | 10 | 26 | 5 | 45 |

**感染者・濃厚接触者の発生に備えた退職者や経験者の動員は3割弱で検討を含むと6割弱**
**業務の専門性の高さが関係し、他のプラントからの支援は、あまり検討されていない**

# 操業現場での感染防止策

## 一般的な運転員の感染防止

手洗い消毒、マスク、フェースシールド、ビニール手袋、防護服の装着、
デスク回りの消毒

会食禁止、県外移動の制限

## 一般的な職場の感染防止

動線隔離、パーティション、会議室等人数制限
換気の強化、空気清浄機の追加

黙食、食堂の着席制限、更衣室の使用禁止（作業服通勤）、工場内浴場の使用禁止

時差通勤、公共機関での通勤回避（レンタカー通勤や工場内に宿泊する例も）

寮や社宅での感染者の隔離場所の確保を回答している例も

## コントロールルームの感染防止

入室制限、引継ぎ会議のリモート化、

テレビ電話やウェアラブルグラスでの作業指示

タッチパネルの消毒、アクリル板等の設置、制御コンソールの配置変更

予備のコントロールルームの利用という回答も10件（2割以上）あった。

# 感染者の入構防止と接触者追跡

**新型コロナウィルスでは、症状がないまま感染を広げる保菌者が存在し、**
**検温と検査で発症者は特定できても、感染者は特定できない。**

## 発症者の入構防止と接触者追跡

検温、入退室管理、在勤時の滞在場所と接触者の記録管理（1割が勤務時間外の行動記録を要求）

来訪者には、来訪後の発熱等の症状が発生した場合には連絡するよう依頼

対人接触履歴追跡システム（COCOAの利用を挙げたのは2件であった）

事前PCR検査（調査時期もあり、回答数は2と少なかった）

## 体調管理

毎日の体温測定と記録

体調不良者のデイリー報告・情報共有

感染者・濃厚接触者の復職ルールの策定

感染防止教育や家族への協力依頼は6割以上が実施している

（短期的には家族との接触を制限したとの回答も1件あった）

# 現場作業での感染対策

## 三密回避が困難な作業の感染防止

| | 中長期的に適用 | 短期のみ適用 | 検討したが実施していない | 検討していない | 無回答 | 合計 |
|---|---|---|---|---|---|---|
| 不急作業の延期，中止 | 7 | 22 | 3 | 10 | 3 | 45 |
| 作業および確認項目の削減による時間短縮 | 6 | 13 | 4 | 19 | 3 | 45 |
| 作業の効率化による時間短縮 | 13 | 10 | 4 | 15 | 3 | 45 |
| 作業の効率化による現場人員の削減 | 6 | 9 | 12 | 15 | 3 | 45 |

- **機械化・自動化投資による作業時間・**
- **作業の効率化はリモート支援など、機械化・自動化による人員削減も**
  **作業期間の延長による１日あたりの作業員数の削減という回答も**
- **エアラインマスクによる作業という例も**

## リモート支援による現場運転員の業務担当

| | 中長期的に適用 | 短期のみ適用 | 検討したが実施していない | 検討していない | 無回答 | 合計 |
|---|---|---|---|---|---|---|
| リモート支援によるトラブル解析 | 4 | 2 | 11 | 24 | 4 | 45 |
| リモート支援による修理・更新作業 | 6 | 3 | 8 | 24 | 4 | 45 |
| リモートからの遠隔作業の実施 | 6 | 3 | 7 | 25 | 4 | 45 |

**2割程であるが、トラブル解析、修理・更新作業、遠隔作業などが実施されている**

# リモート支援に利用された方策

| 複数回答可 | 回答数 |
|---|---|
| 通信回線の設定 | 4 |
| 支援用アプリ | 0 |
| テレビ会議アプリ | 9 |
| スマートフォン | 4 |
| ウェアラブルカメラ | 9 |
| 防爆タブレット | 4 |
| 検討はしたが、実施困難 | 3 |
| 検討していない | 9 |
| 無回答 | 17 |
| 合計 | 59 |

**コロナ禍で検討したのではなく、従来から競争力強化のために検討していたものが、有効に働いたというコメントが多い。**

**上記数字は、現場の支援という設問に対しての回答数で、テレビ会議システムは、ほとんどの回答者が利用していると考えられる。**

**他に、AR（拡張現実）を検討中という回答があり、ドローンの利用も進んでいると考えられる。**

# 接触回避とコミュニケーション不足

| | 中長期的に適用 | 短期のみ適用 | 検討したが実施し | 検討していな | 無回答 | 合計 |
|---|---|---|---|---|---|---|
| 直引継ぎや作業打ち合わせを構内同士でテレビ会議 | 16 | 6 | 1 | 18 | 4 | 45 |
| 直引継ぎや作業打ち合わせを電子ファイルで効率化 | 25 | 1 | 2 | 13 | 4 | 45 |
| 在宅勤務者や外部業者とテレビ会議で打ち合わせ | 24 | 8 | 0 | 7 | 6 | 45 |

**対面の機会は減った**

| | 感じている | 短期的には感じた | 感じない | 無回答 | 合計 |
|---|---|---|---|---|---|
| コミュニケーション不足の発生の危惧 | 15 | 12 | 11 | 7 | 44 |

**6割が、コミュニケーション不足を危惧している**

**リモートでも回数を増やしたり、カメラで顔色がわかるようにしたり、
パーティションでの対面機会を増やしたり、
電子システムの導入で、情報を共有を確実にしたり、
工夫をしている。**

# 定期修理での感染防止策と課題

## 感染防止策

- 作業用プレハブや作業受付テント、トイレ、屋外喫煙所の**増設・分散**
- 受付や休憩所でのパーティションの設置
- 電子受付や時間差による入場、作業**時間・箇所の分散**、食事時間・場所の分散
- **来場できない**海外や県外の業者の代替調整と作業削減
- 調整員が県外からウェアラブルツールにより、**リモートで保守支援**
- 感染症対策と**熱中症対策の両立**（マスクをはずしてよい条件の明確化）
- 入場者の事前2週間の**体調管理と行動ルール**の事前連絡の要請

## 課題

- 工事着工許可の電子申請化や朝礼、作業打ち合わせの削減、リモート化で、
  **士気の低下、安全指示事項や意思疎通などの欠落**が危惧されるという回答も
- 立会検査ができず、時間差でチェック　単独作業の発生は**防犯上の問題**に
- 防護具着用で**作業性悪化**
- 県外の作業者の大量流入に対する**地域住民や監督官庁との折衝・調整**
- 宿泊所から外出制限などの自粛要請の周知徹底
  **近隣住民から、作業員が飲食に出歩いている等のクレーム**があり、その都度協力会社の協力要請した。
- 工事用部材の**調達**に、納期長期化が発生し、入手できないものが発生

# 経済産業省の定期修理の弾力的運用措置

## 経産省は2020年4月保安検査及び定期自主検査の期間延長措置を発表

| 複数回答可 | 変更なしで実施 | 変更し実施 | 延期あるいは中止した | 検討はしたが実施困難 | 検討していない | 無回答 | 合計 |
|---|---|---|---|---|---|---|---|
| 回答数 | 26 | 8 | 2 | 1 | 2 | 9 | 48 |

回答者のうち，**6割**が定期修理の実施時期を変更することなく実施している．
時期を変更したところが**約2割**あったが，延期・中止は**2件**に留まった．

| 複数回答可 | 調整がしやすくなった | 調整には時間不足 | 有効で，今後の継続も希望 | 無回答 | 合計 |
|---|---|---|---|---|---|
| 回答数 | 3 | 10 | 11 | 21 | 45 |

弾力的運用の有効性については，「調整には時間不足」との回答が**約1/4**あったが，その他は「調整しやすくなった」と「有効で今後の継続を希望」をあわすと回答の**約3割**であった

**経済産業省（高圧ガス）と厚生労働省（ボイラー・一圧）**で，
検査有効期間の起算点の取り扱いに差があり，本年度弾力的運用を行った施設において，
**次年度の定期修理の時期設定が難しくなっている**との回答もあった

# BCP（業務継続計画）

- 新型インフルエンザ等対策特別措置法(2012年)「特措法」により、
  事業者においては、業務継続計画の作成が求められている。
  今回のCOVID-19に対して、既存のBCPが有効性と
  次なるパンデミックへの備えとしての課題を調査した。

| 複数回答可 | 回答数 |
|---|---|
| 地震 | 39 |
| 台風 | 23 |
| 津波 | 27 |
| 新型インフルエンザ | 20 |
| その他 | 5 |
| 合計 | 114 |

地震のBCPは**大多数の事業所**が策定しているが、

新型インフルエンザのBCPは
特措法で求められているのに、
**半数に満たない**

## COVID-19で意識されたリスク

**集団感染（クラスター）による人員不足**のリスクに関する回答がほとんどで、

- 当該プラント及び関連プラント（用役，前処理関連）の**操業停止**の回答が多い。

それ以外に、下記のような回答がみられた。

- **装置の安全な停止や保全への影響**
- **サプライチェーンへの影響**
- **労働災害の発生**
- **他への技術者の派遣困難**
- **風評被害，企業イメージ低下の怖れ**

## 既存のBCPが有効だった点

| | 有効だった | 不足していた | 策定していなかった | 無回答 | 合計 |
|---|---|---|---|---|---|
| プラント停止や操業条件、操業体制の見直し | 15 | 4 | 9 | 17 | 45 |
| 顧客等周辺関係者との連携 | 15 | 3 | 7 | 20 | 45 |
| サプライチェーンでの変化に対する対応 | 13 | 4 | 8 | 20 | 45 |
| マスクの確保などの感染予防対策 | 25 | 6 | 4 | 10 | 45 |

**上記の対応を別のBCPにおいてでも検討されていたら、有効に働いたと考えられる。**
在庫管理の観点、SARS,MARSでの経験で、マスク不足に対応できたという例もあった

## 既存のBCPでは不足だった点

| | 中長期的対応 | 短期的対応 | 無回答 | 合計 |
|---|---|---|---|---|
| 感染予防のための職場以外の生活への対応 | 14 | 5 | 26 | 45 |
| 感染拡大や被害の予測のための方策 | 14 | 4 | 27 | 45 |
| 関係各所との連携 | 9 | 6 | 30 | 45 |

- **無回答が過半数である.**
  **既存のBCPでは上記の観点は対応していなかった**と考えられる.
- **新型コロナウィルスの感染に関しては、世界で日本だけが激減しているように、現在も予測が難しい状況である。**
- 地震,水害を想定した備品類備蓄（飲料水,土嚢など）は行っていたが,
  感染予防備品（消毒液,マスク等）の備蓄がなく調達に困難を極めたという回答もあった

# 事業継続に必要な観点

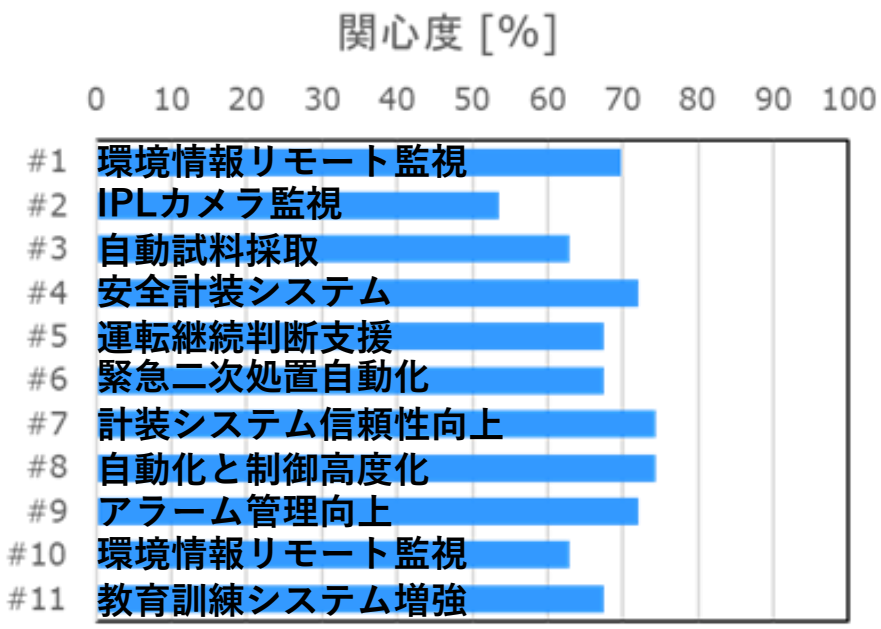
| 複数回答可 | 回答数 |
|---|---|
| サプライチェーンの国内回帰 | 17 |
| できるだけリモートから実施できる体制 | 26 |
| 企業間のより高度な連携 | 11 |
| 想定外のインシデントに対応できるレジリエンシーの向上 | 22 |
| 新たな事業継続計画を実現するための教育 | 9 |
| 無回答 | 5 |
| 合計 | 90 |

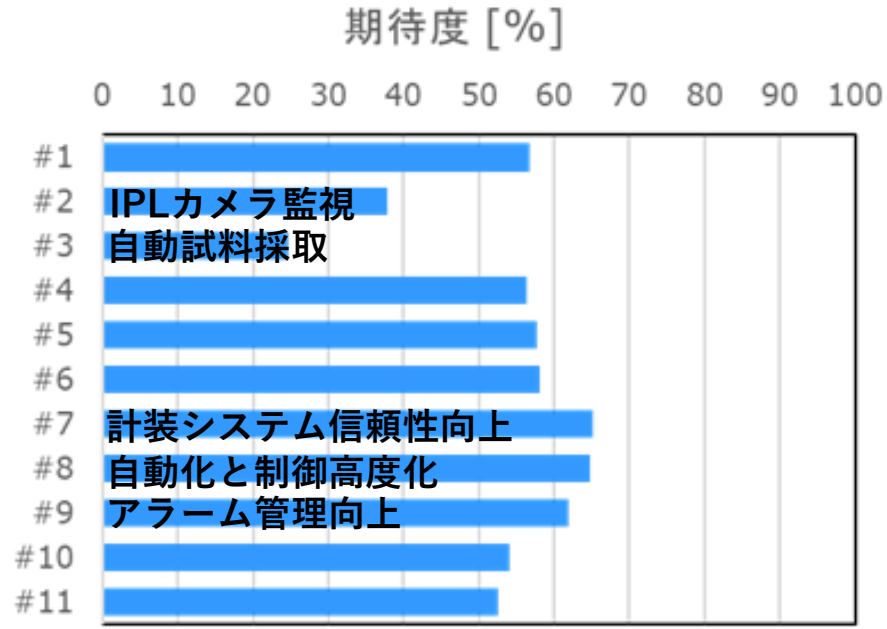
- **感染症**という想定は，インフルエンザ流行時にBCPを策定したところでは，すでに想定したものと考えていると思われる。
- しかし、以前とは考え方,意識も変えた,**中長期的なBCP**を策定する必要があり，リスクの想定範囲や想定状況を広げ,想定外に対する応用力を高める必要がある。今の時点での想定は低い．という回答もある。
- **想定外**の事象と思われたところもある。想定外にも適切に対応できる準備が必要と意識している回答は半数になる。
- **リモート**での業務の必要性を意識している回答が半数を超える。
- 海外に依存しているサプライチェーンの**国内回帰**と**企業間の連携**の必要性についても、回答は多い。

# 従来から期待されていた自動化に関する技術

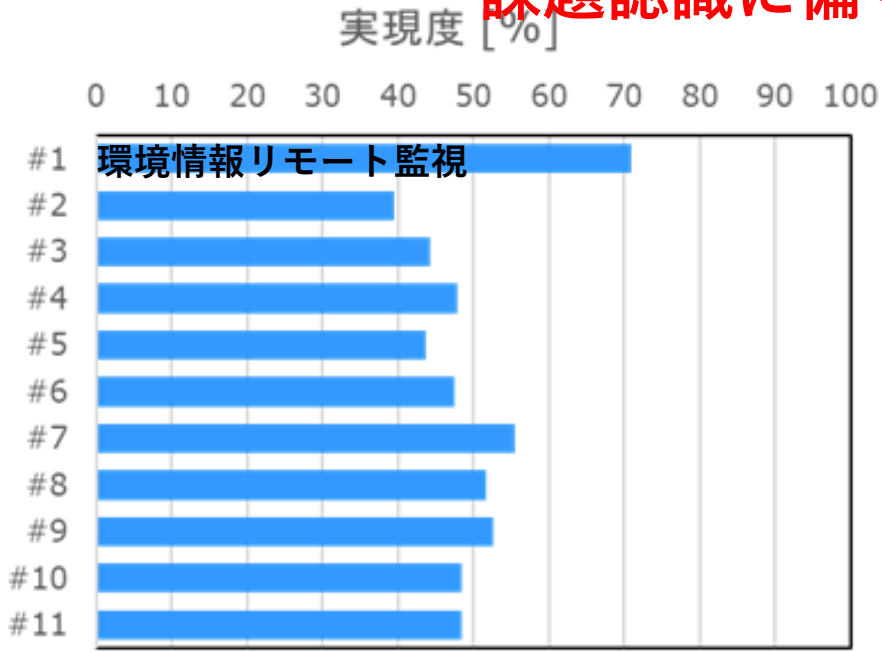
## 運転安定化・運転監視強化・トラブル低減・異常対応的確化などを一層進めて，少ない陣容でも不測の事態に対処できる体制への期待が高まっているか調査した。

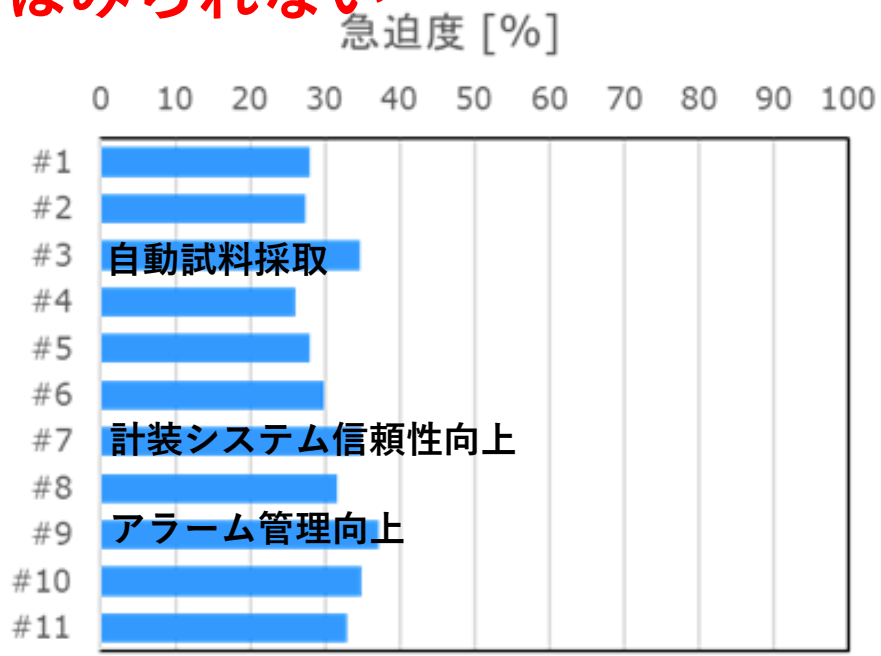
| 番号 | 課　題 | 内容事例 |
|---|---|---|
| 1 | 環境情報リモート監視 | 排ガス SOx, NOx・排水PHなどの環境計測情報を遠隔で監視する. |
| 2 | IPL カメラ監視 | IPL多重独立防護層たとえば防油堤をカメラ監視する. |
| 3 | 自動試料採取 | 定周期の工程分析のためのサンプリング作業を自動化する. |
| 4 | 安全計装システム | レガシーなリレーインターロックシステムを最新の安全計装システムに入れ替え信頼性を一段と高めると共に増改造を容易にする. |
| 5 | 運転継続判断支援 | 運転トラブルや設備故障時に運転継続停止の判断（意思決定）を支援するシステムを導入する. |
| 6 | 緊急二次処置自動化 | 緊急停止後の二次処置を極力自動化して人の作業負荷を軽減すると共に誤操作・誤判断の防止を図る. |
| 7 | 計装システム信頼性向上 | さらなる信頼性向上を図る．たとえばセンサー・操作部の故障に対するフェイルセーフ機能を増強する. |
| 8 | 自動化・制御の高度化 | さらなる自動化と制御の高度化により運転作業負荷軽減と運転安定化を図る. |
| 9 | アラーム管理向上 | さらなるアラーム削減や管理方法改良により運転監視作業の負荷軽減と監視強化を図る. |
| 10 | PID 制御性向上 | PID 制御ループ のAUTO率と制御性能を向上してオペレータを介入調整から解放し運転安定化を図る. |
| 11 | 教育訓練システム増強 | 休暇を取る人の代務ができるように，VR，AR などを利用して定期的にクロストレーニングするシステムを導入し運用する. |




課題認識に偏りはみられない



# 従来から期待されていた自動化に関する技術の評価

1. **コロナ禍を逆に好機と捉えて積極的に課題解決する活動には至っていない.**
2. **課題解決を阻害する要因のトップに低投資効果**が挙げられた.
3. **計装システム信頼性向上、自動化と制御高度化、アラーム管理向上への関心が高い.**
   解決策が明確になっており事例も豊富なこれらに親近感があるのだろう.
4. **緊急停止後の二次処置自動化、教育訓練システムに対する期待が盛り上がりに欠けた**のは意外だった.
5. われわれの現場体験からの予想がはずれ，**PID制御性能への関心が低い.**
   現場の実態把握が不十分なのかもしれないし,
   AI, Big data, IoT等の流行している魅力的な分野に影響されているのかもしれない.
6. 技術増強が必要な分野として，**運転継続判断支援、計装システム信頼性向上、自動化と制御高度化、アラーム管理向上**が挙げられた.
   これらに関する有用な実用技法や実施事例を回答者にフィードバック提供できるよう報告書にリンクを示している.

# 現状課題への提言

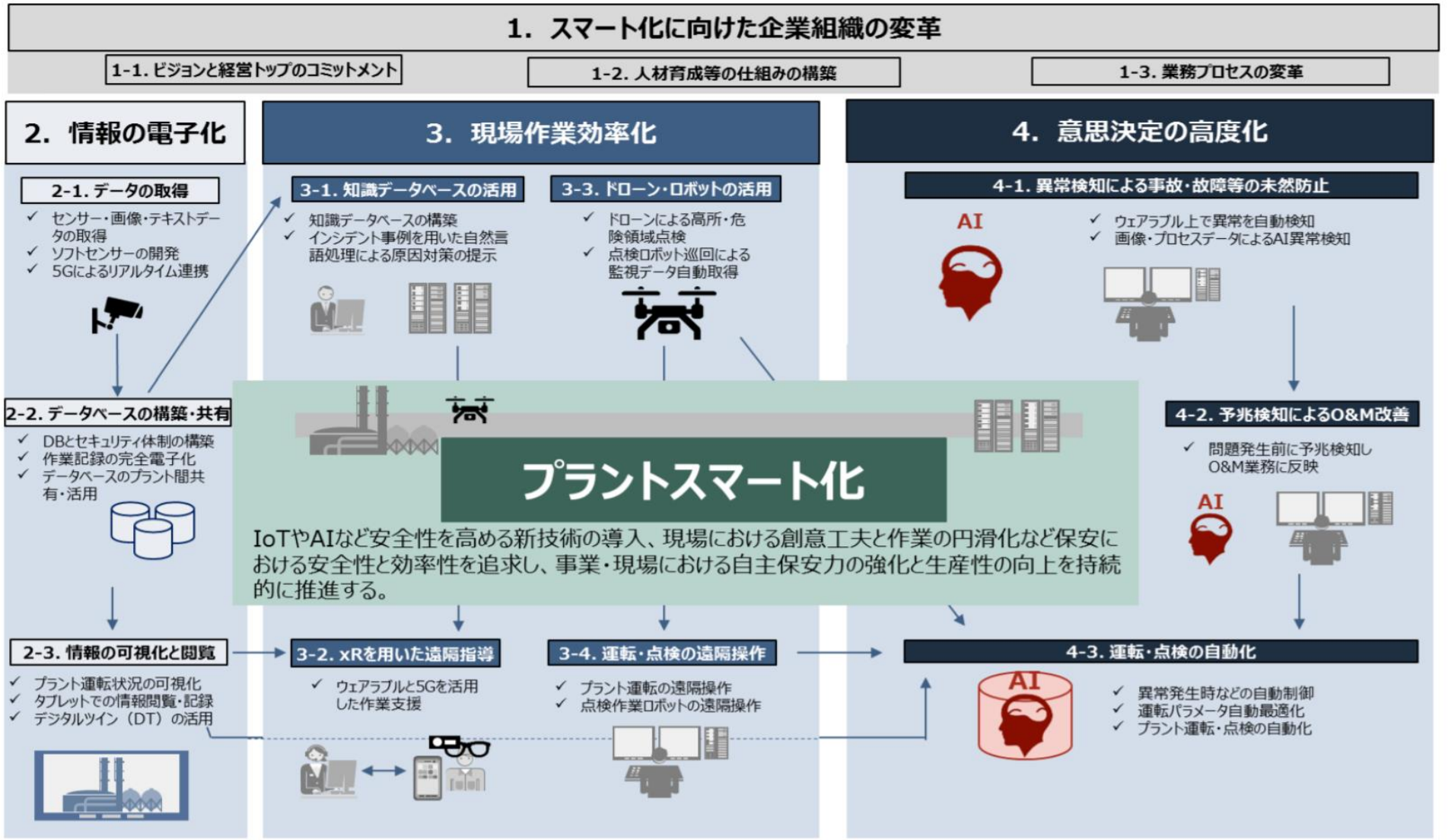
- ここで挙げた課題解決のためには二通りの取組が必要であろう.
  **第一は，日常的な改善活動を地道に取り進めることである**.
  　大きな投資を要せず自主解決できるテーマを実践することである.
  **第二は，大きな投資を要するテーマを実行することである.**
  　効果を定量化することが困難な緊急停止後の二次処置自動化であっても,
  　その必要性を認知させ段階的に実行していく取り組みにしたい.
- 計測制御情報システムのベンダーには，アンケート結果をレビューして
  **新しい製品開発やサービス展開**を図ってほしい.
  　たとえば，自動化の一般的な方法と費用の指針を作成して公開するとか,
  　調節弁スマートポジショナーにフェイルセーフ機能を付加するなどが
  　考えられる.

# 将来技術への期待に対するコロナ禍で変化

## 経産省 スマート保安アクションプラン（案）の25項目で質問

## スマートプラントにおける将来技術

2020年7月 スマート保安官民協議会 高圧ガス保安部会



# 将来技術（スマート保全）への期待

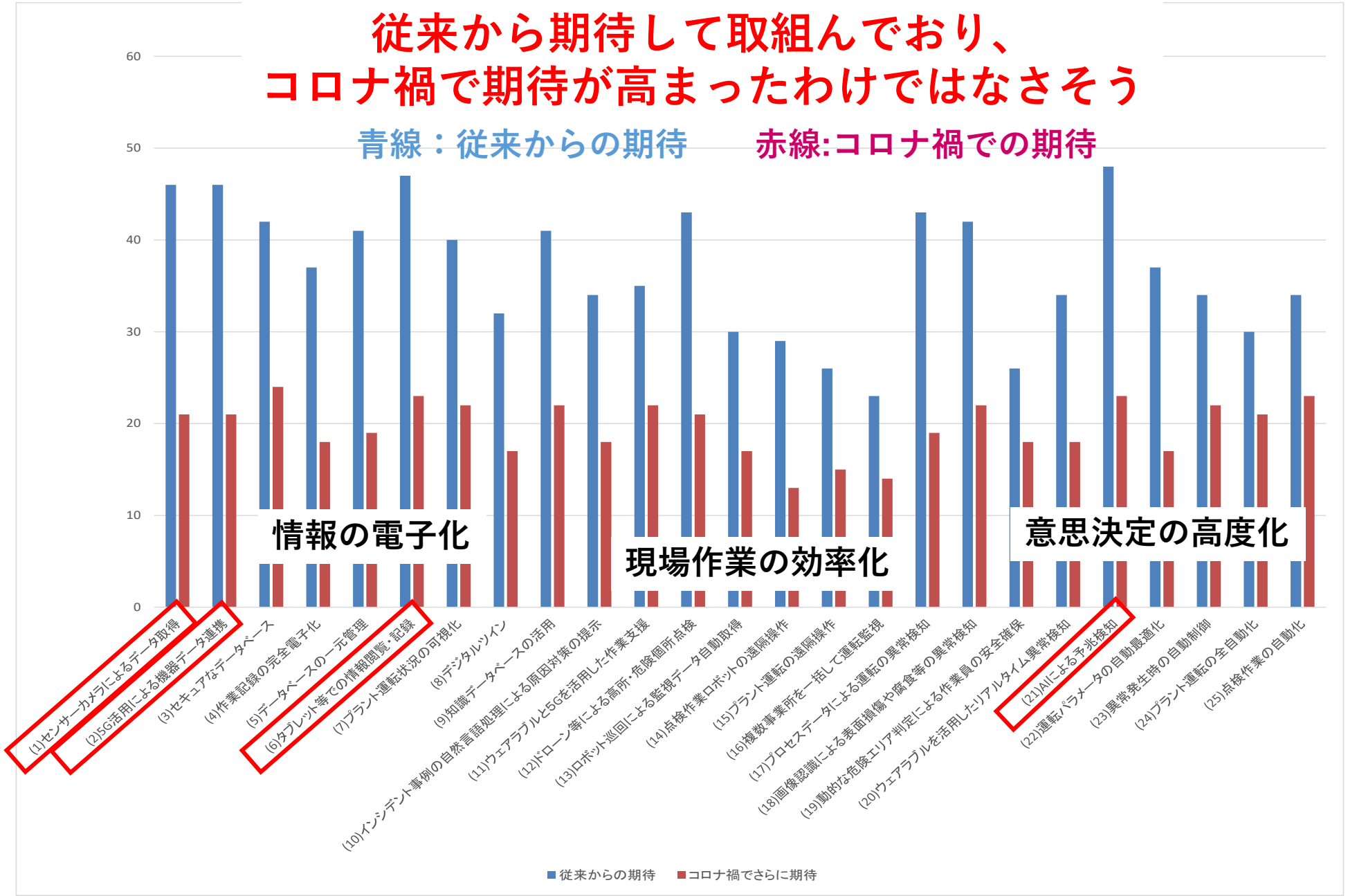
| 区分 | 分類 | 実用化が期待される技術・システム | 番号 |
|---|---|---|---|
| 情報の電子化 | データの取得 | センサーカメラの設置によるデータの取得 | 1 |
| | | ５G等を活用した機器データのリアルタイム連携 | 2 |
| | データベースの構築と共有 | セキュリティが確保されたデータベース構築 | 3 |
| | | 引継ぎノートを含む作業記録の完全電子化 | 4 |
| | | データベースのプラント間接続と情報連携による一元管理 | 5 |
| | 情報の可視化と閲覧 | タブレット等での情報閲覧・記録 | 6 |
| | | プラント運転状況の可視化 | 7 |
| | | デジタルツインによるシミュレーションと状態可視化 | 8 |
| 現場作業効率化 | 知識データベースの活用 | 知識データベースの活用 | 9 |
| | | インシデント事例を用いた自然言語処理による原因対策の提示 | 10 |
| | XR を用いた遠隔指導 | ウェアラブルと５Gを活用した作業支援 | 11 |
| | ドローン・ロボットの活用 | ドローン等による高所・危険個所点検 | 12 |
| | | ロボット巡回による監視データ自動取得 | 13 |
| | 運転・点検の遠隔操作 | 点検作業ロボットの遠隔操作 | 14 |
| | | プラント運転の遠隔操作 | 15 |
| | | 複数事業所を一括して運転監視 | 16 |
| 意思決定の高度化 | 異常検知による事故の未然防止 | プロセスデータによるプラント運転の異常検知 | 17 |
| | | 画像認識による表面損傷や腐食等の異常検知 | 18 |
| | | 動的な危険エリア判定による作業員の安全確保 | 19 |
| | | ウェアラブルを活用したリアルタイム異常検知 | 20 |
| | 予兆検知による運転・保守改善 | AIにより問題発生前に予兆検知し運転・保守業務に反映 | 21 |
| | 運転・点検の自動化 | (a)運転パラメータの自動最適化 | 22 |
| | | (b)異常発生時の自動制御 | 23 |
| | | (c)プラント運転の全自動化 | 24 |
| | | (d)点検作業の自動化 | 25 |

**評価項目：**

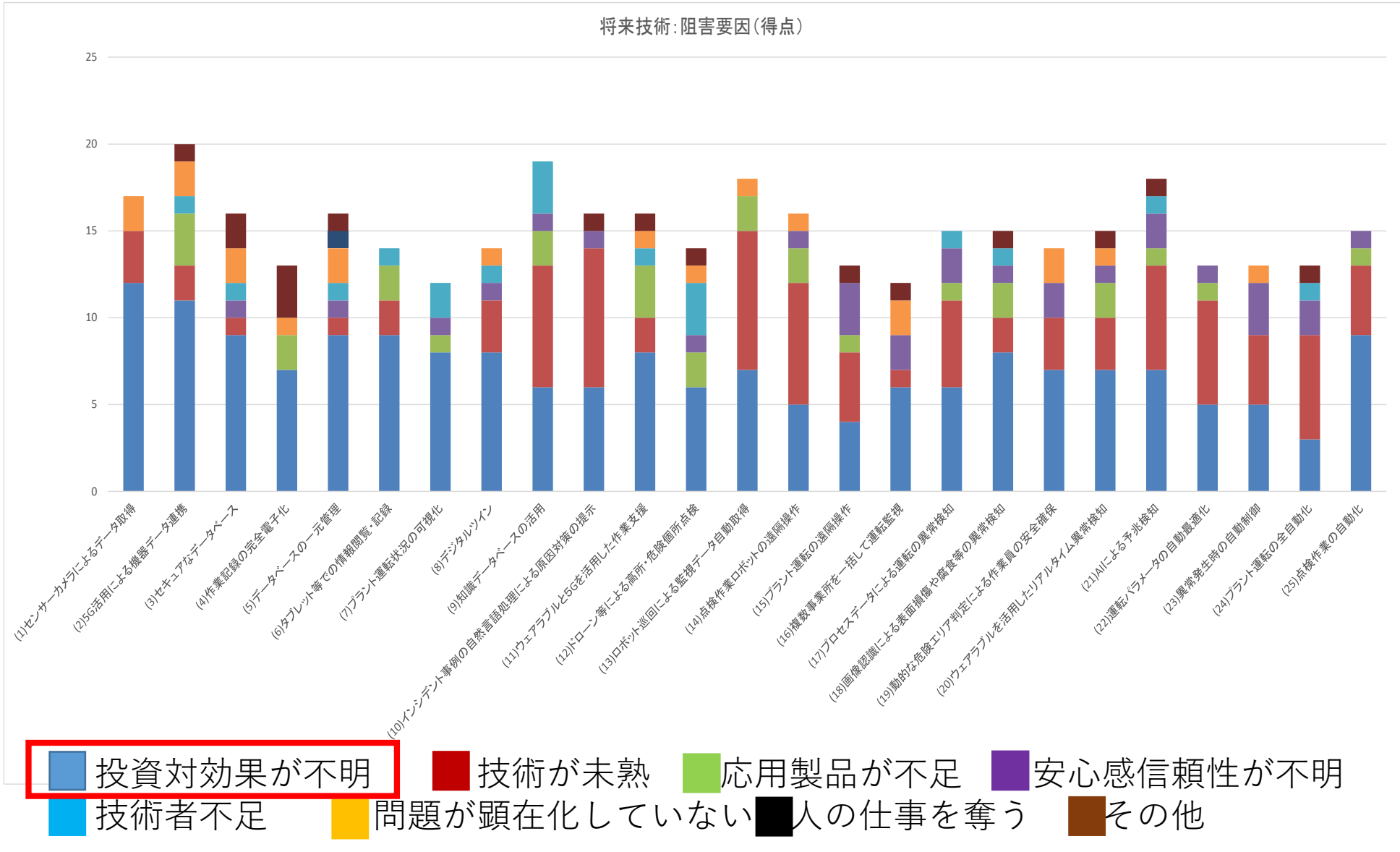
- 従来からの期待
- コロナ禍でさらに期待
- 取組状況
- 期待する実現時期
- 阻害要因

**情報の電子化**
**８項目**
**現場作業の効率化**
**８項目**
**意思決定の高度化**
**９項目**

# 将来技術への期待がコロナ禍で大きくなった？



# 将来技術の阻害要因の回答には、無回答が多いが、低投資対効果が多い



# 将来技術への提言

1. **AIや自動制御**に関する項目に技術的課題があることを多くから指摘された.
   さらに，**ウェアラブルと５Gを利用した点検**なども,
   計測自動制御学会が深く関係する分野であるので,
   **学会が勉強などの機会を提供する**ことが有効であると考えられる.
2. 将来技術の導入には防爆対策が問題になることが多いので,
   **防爆技術，法規制**の緩和についても,
   **学会や業界団体と共同**で検討するという活動も望まれると感じた.
3. **ビジネスプロセスの変革や新たなサービスの創出とかのDX**につながるような将来技術の議論は，アンケートではあまりできなかったが,
   将来技術に対して，このような観点の議論も進めることが望まれる.
4. 将来的には，**プラント自体にも変革があるという将来ビジョン**も必要である.
   従来は大型化により効率化を図ってきたが，小型化・並列化・パッケージ化で，管理を容易にし，フレキシビリティを高め，無人化を推進することも考えられる.
5. さらに，将来技術には，**産業構造自体が変化する可能性まで考慮**する必要があるとも考えられる．ここでは，アンケートを基にした提言ということで，そこまでの議論は避けるが，温暖化ガスゼロ排出で電気自動車化の動きが加速しているなど，社会の動きも考慮した大きな視野での議論に展開する機会になることを期待する.

# Connected Worldでのプラント操業

**少ない高度技術者による高度な操業**

現場は低い専門性でも操業可能

（遠隔から作業員に着目点を指示し、画像で作業を管理）

**高度な外部連携**

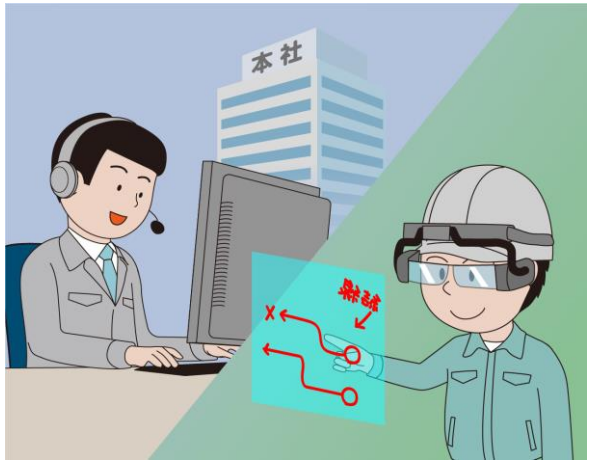
- タイムリーで適量の製造
- 新たな需要の創生と
  新たなサービスへの参画

（人工呼吸器や防護服の製造等）

**世界3か所での昼勤で世界中の24時間操業を実現**

**必要な技術**

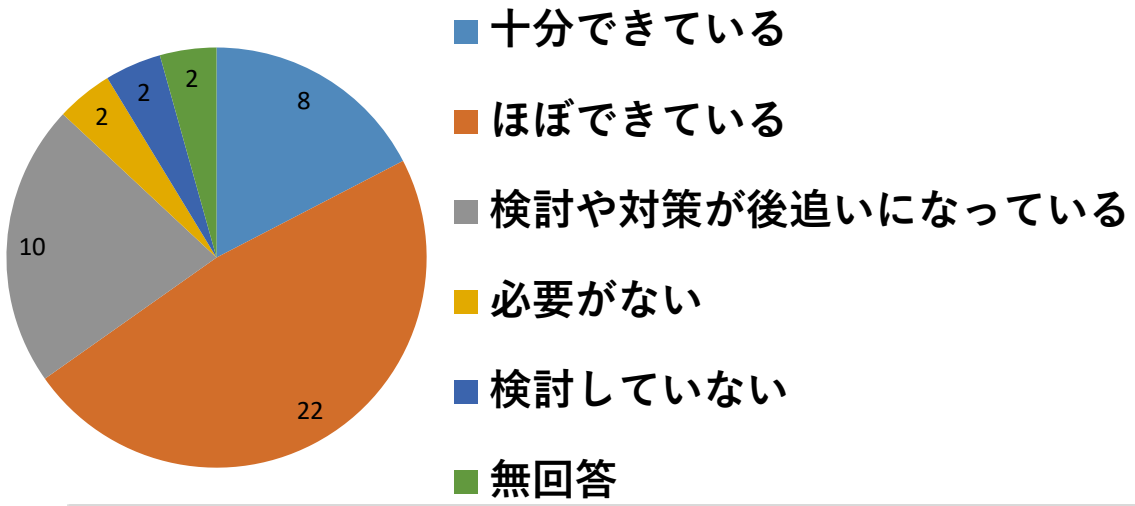
・現場技術者の支援
  ・ウェアラブル端末
  ・拡張現実
  ・標準化
・現場の自動化・少人化
  ・ AIによるサポート
  ・防爆ロボット、ドローンの活用




https://smartfactory.tn-japan.co.jp/solution_work/

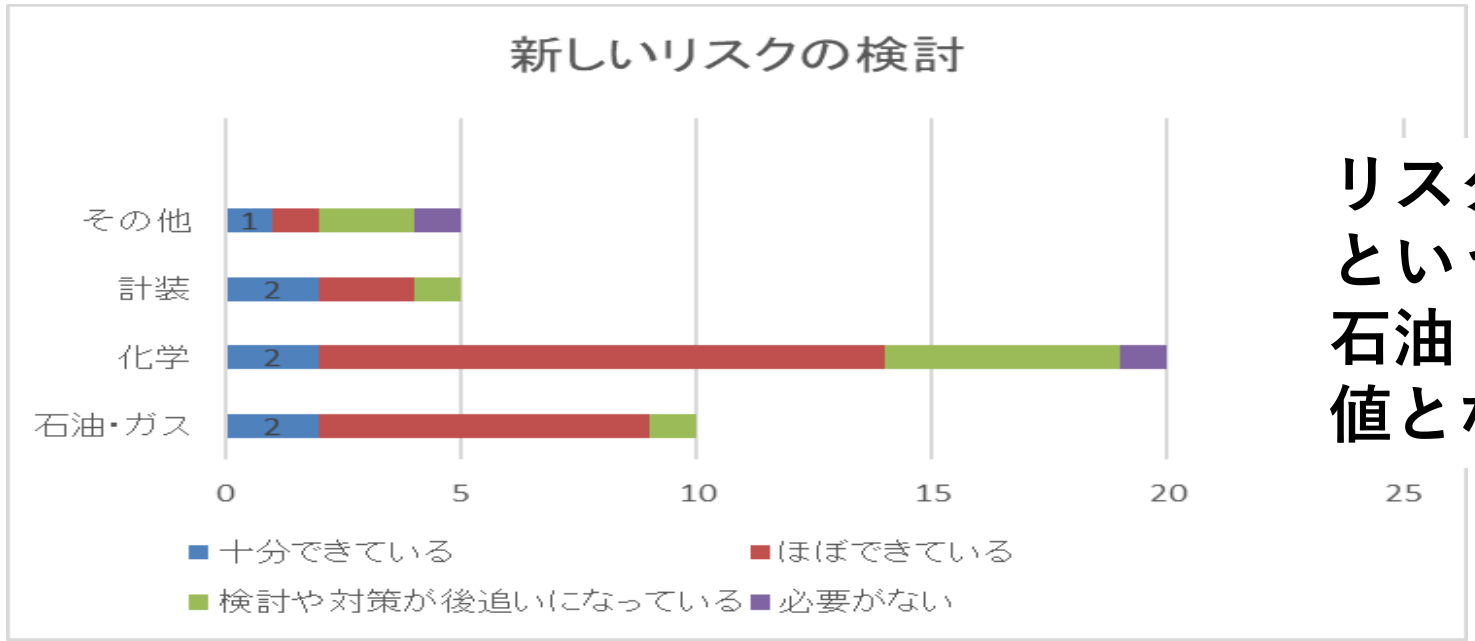
# セキュリティに対する意識調査①

## 新しいセキュリティリスクの評価



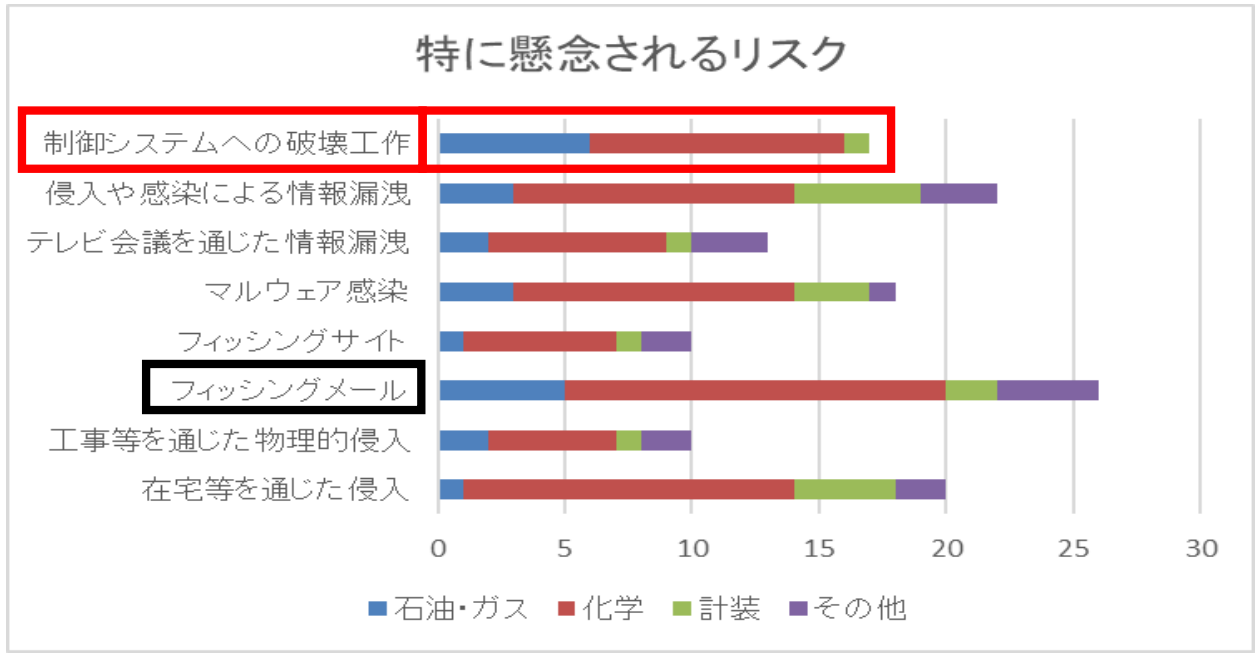

コロナ禍で、在宅勤務やリモート会議が進展し、サイバーセキュリティへの意識は高くなっているし、実際に検討をしていると考えられる

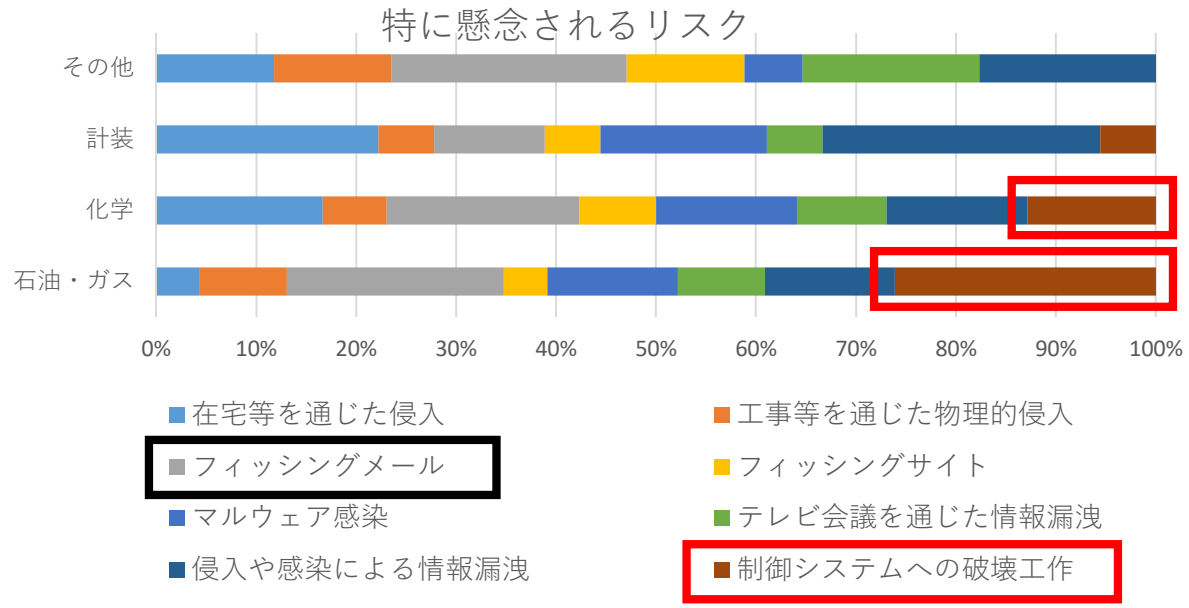
ただ、サイバーセキュリティの検討に対して、十分できているという評価は回答者が専門的に評価したものとは限らないので、その意識が安心できるものか、追調査が必要かもしれない




リスクの評価ができているという回答率は
石油・ガスと計装で高い数値となっている

# セキュリティに対する意識調査②

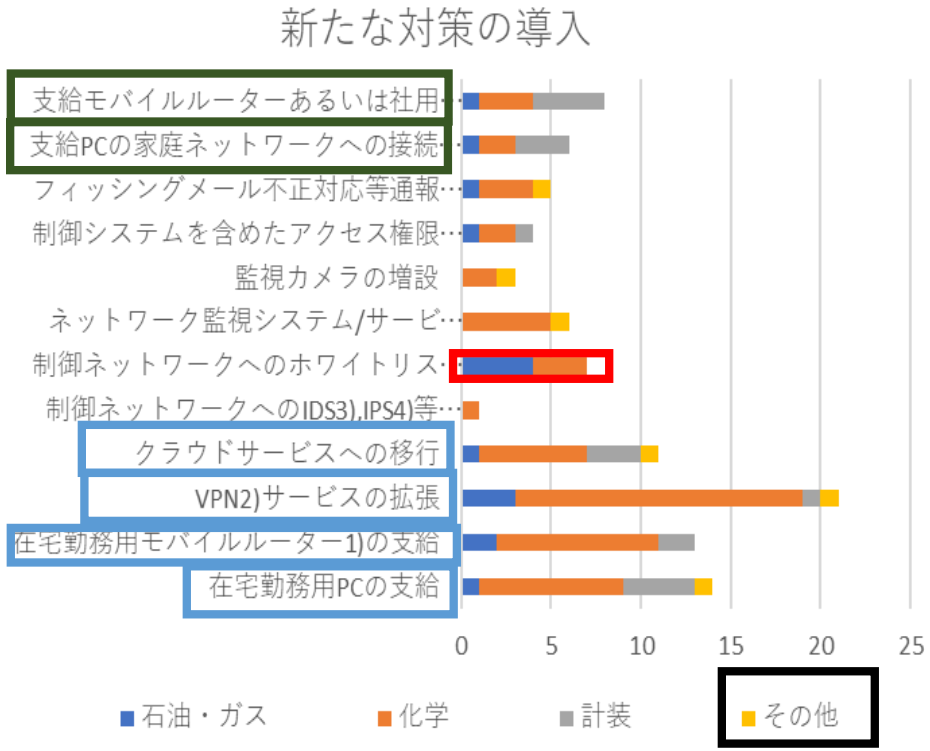


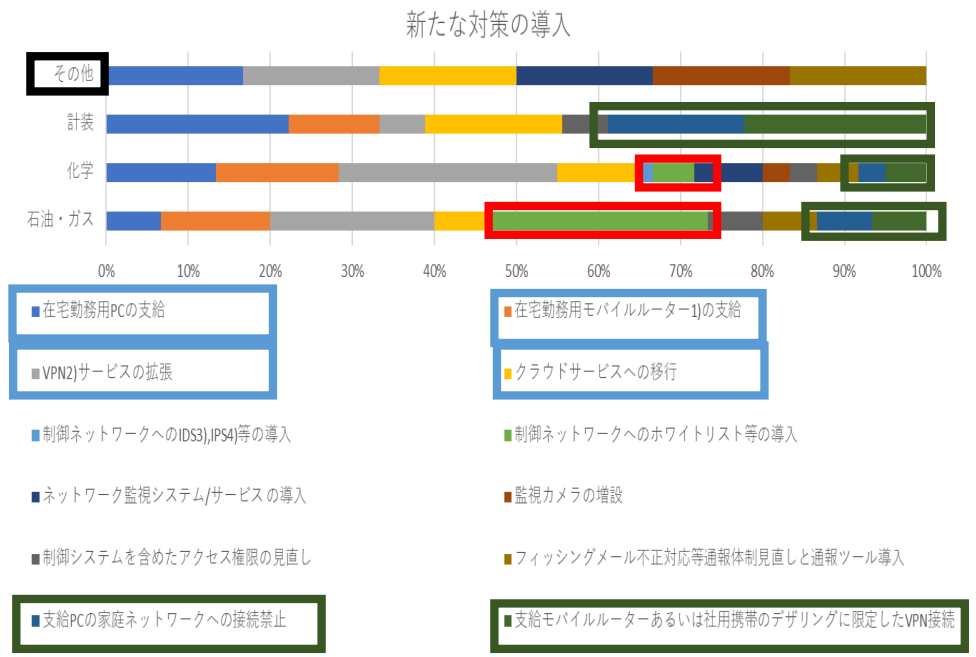




様々なリスクが懸念されており、
コロナ禍での給付金等に関する詐欺が
増えているので
フィッシングへの懸念も
全業種で表明されている。

石油ガスや化学では、
制御システムへの破壊工作が
高く意識されている。

# セキュリティに対する意識調査③




**コロナ禍で、半数以上が新たな対策の導入を検討している**

**VPNの拡張が最も多く、在宅用PCやモバイルルーターの支給、**

**クラウドサービスへの移行を行っている事業所が多い。**

**半数以上が、コロナ禍を機会にセキュリティポリシーを見直している。**

**石油ガス・化学では、ホワイトリスト等、制御ネットワークへの対策も実施。**

**コロナ禍で在宅勤務やＷＥＢ会議が急速に進展したが、**

**在宅からの被害を警戒して、家庭用LANとの接続を禁止している例も多い。**

**ただ、その他が石油ガス、化学、計装に比べると意識が低いことが推定される。**

# コロナ禍でのサイバー攻撃のリスク

**コロナ禍で、リスクは増大している**

- 一人作業が増えている？

  作業員とともに、攻撃が侵入。
  発信機設置や不正プログラムを組み込まれるリスク
- 在宅勤務で家庭での感染から侵入
- フィッシングサイトから侵入
- リモート接続のVPNの脆弱性などから侵入
- もともとアンチウィルスの検知率は低い
- SIS（安全計装）にもサイバー攻撃のリスク

**2021年5月アメリカ大統領令**

**ゼロトラストアーキテクチャーの導入を指示**

**信頼できるネットワークゾーンは存在しない。**
**すべての通信・データに多要素認証と暗号を**

**十分なセキュリティ対策って本当？！**

**コントローラがサイバー攻撃にあうと、**
**監視画面には変化が現れないまま、**
**プラントが危険になりうる**
**ことをリスクとして認識すべき。**

# 【第2部】

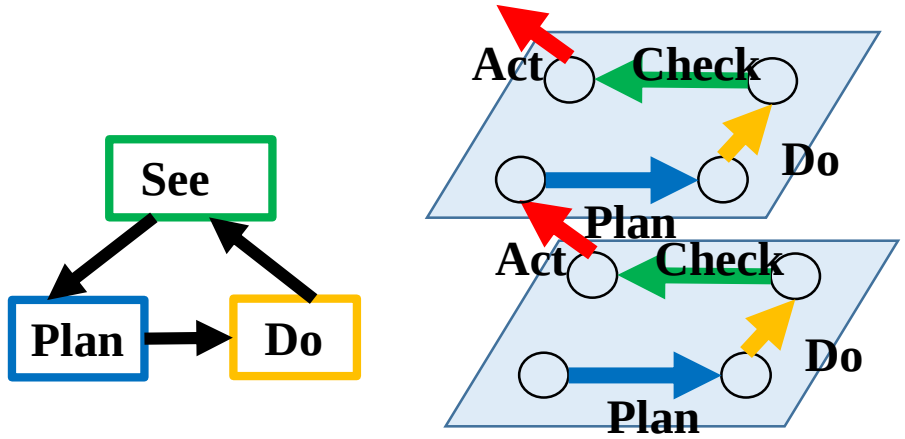
# リモートが進んだ状況下での
# サイバーセキュリティ

# ここからの話の要点

- プラントでは安全第一、次に事業継続
- セキュリティ対策はきりがない
  - 安全確保には拠り所をもちたい
  - ツールより組織・体制が大事
- 特に上・下・外部をうまく機能させる中核人材
  - 経営者はその中核人材の仕事を理解し任せる
  - **企業は、プロの集団。**自分の得意を高めるとともに連携しあって、より**組織を成長**させる
  - サイバーセキュリティの普及・啓発は**知識ではなくリスク意識**（課題の共有）
  - だれかがやればよいのではなく、みんなが意識しないと守れない（安心はありえない）
  - **PDCAのスパイラルアップ**で100点ではなく新たな創造（想像）をめざす
  - Actの見える化（**全員で考え、共有**）のための**演習**

NIST CSF（Cyber Security Framwork）

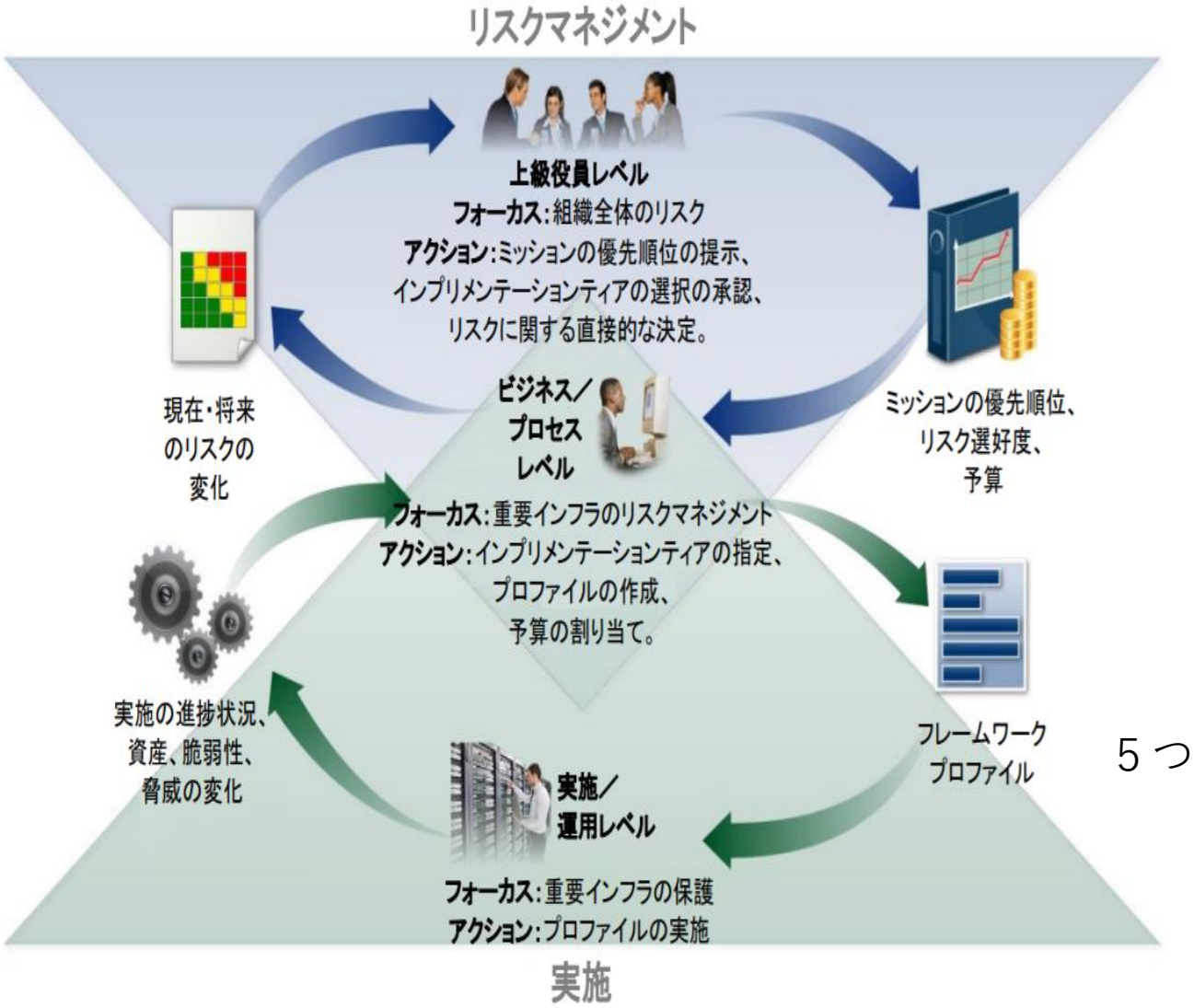

みんながわかる言葉で課題共有




確実にするのではなく、創造性を高める

# NIST CSF(Cybersecurity Framework)

- まず話題のまとめで現れるNIST CSFについて説明する。




2013年にオバマ大統領により発行された
大統領令に従い， NIST(米国標準技術研究所)から
2014 年にver.1.0が提案され、
2018年にver1.1が公開された
「Framework for Improving Critical Infrastructure Cybersecurity」となっているが、
重要インフラに限らない内容

**中核人材チーム**が経営層と実働部隊の間で、
安全も含めたセキュリティの向上のための
２つのPDCAサイクルを廻す構造で
セキュリティ対策を５つのコアに分類して
ティア1~4という4段階で推進を計画管理する
という基本的な取り組み方を示す

５つのCore：Identify, Protect, Detect, Respond, Recover


セキュリティの専門用語ではなく、
効果がイメージしやすい必要な対策の表現

# CSFの5つのコア(Identify, Protect, Detect, Respond, Recover)

- **Identify（特定）**

  彼を知り己を知れば百戦して殆うからず。
  彼を知らずして己を知れば一勝一負す。
  彼を知らず己を知らざれば戦う毎に必ず殆うし(孫氏の兵法)　**現状はこれでは？**

  **Identifyではリスクを認識することが最重要**

  （彼）OSINT(Open Source Intelligent)とよばれる活動がある。
  ダークウエブやブラックサイトでのサイバー攻撃者間の取引情報や、
  サイバー攻撃の対象となる脆弱性の発生情報、攻撃ツールの開発状況などを様々なツールを利用しながら探る。**この能力を有している企業は稀有**

  （己）自分のセキュリティレベルを理解する。
  攻撃対象が社内にどれだけ存在し、どんな規模の被害が発生するか？
  防御策はどれだけ適用されていて、その脆弱性管理はしっかりできているのか。
  もし攻撃にあったら、どんな形で検知でき対応し復旧できる体制になっているのか？
  そこには、課題はどれだけあり、今後、どうする予定なのか？

# サイバーセキュリティ対策の話題(1)

## サイバーセキュリティのあるべき姿とは？

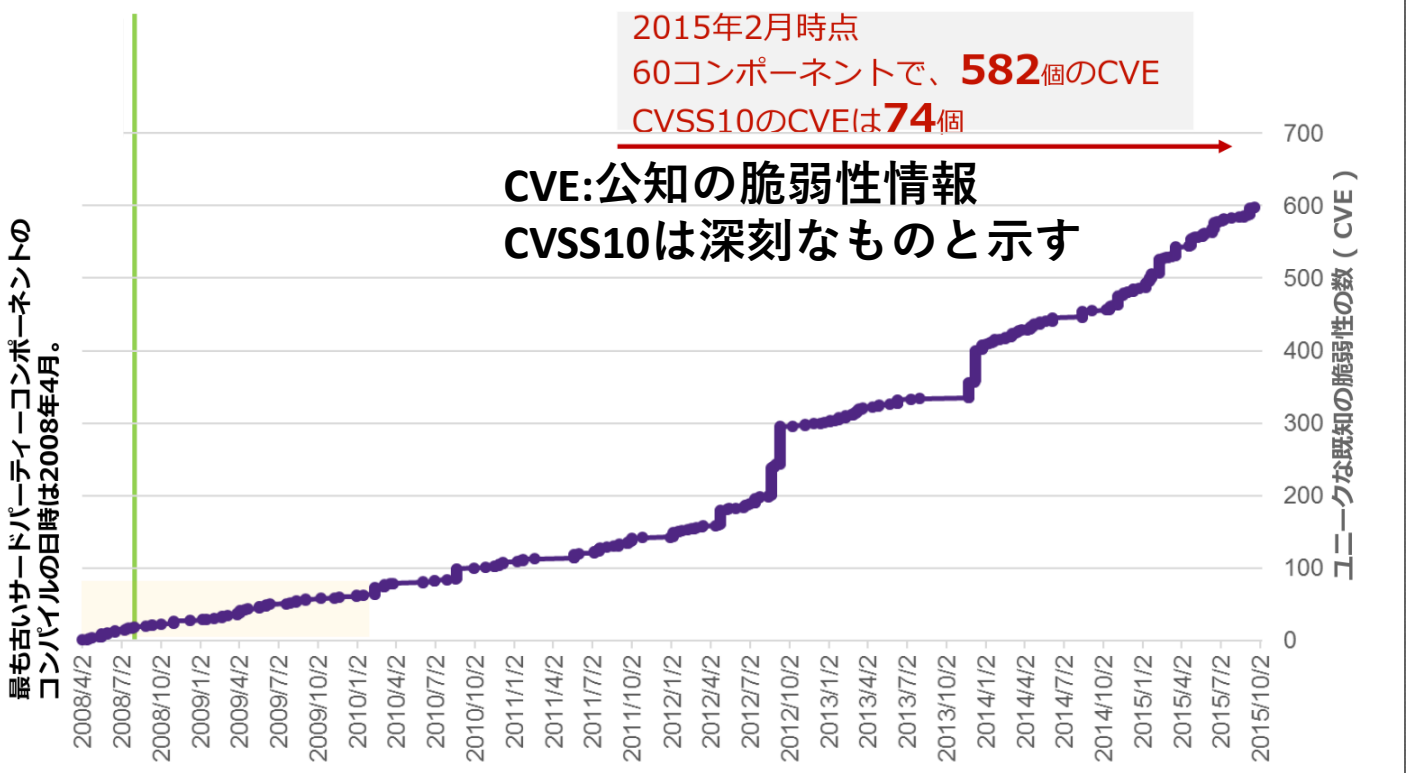
- **どれだけやっても十分になることはない！**
  - **常に新たな脅威が現れ、対策の有効性は保持されない。**
  - **投資を増やせばセキュリティが向上するわけではない。**
    - **運用が大事であり、保守対象が増えると残存脆弱性のリスクは上がる。**
- これだけやっておけばよいというレベルが示されることもない。
  - 人並みにしておけばインシデントが起こっても許される？
    - 社会的な許容というのは状況によって変化する
    - 何が人並み？みんながやっていなければ、自分もやらなくてもいい？
    - **被害が発生しても、事後の姿勢が評価されて、株価がかえって上昇した例もある**
  - 人並みってガイドラインに従えばいい？
    - ガイドラインは着眼点を示しているだけで、それをすればよいというレベルは示されていない。
    - そもそもガイドラインは業界のほとんどの業者が実現できることしか書けない！

# サイバー攻撃の対象は脆弱性を増えつづけている

**脆弱性は攻撃者の発明品**と考えるべきで、セキュア開発しても、
脆弱性はすごいペースで現れる。ましてや、通常のソフトウェアなら？

- 商用の製品
- 81個のサードパーティーコンポーネントを利用
- リリース当時のコンポーネントは、ほぼクリーン

- 平均で5日間に1つの新しい脆弱性が製品のコンポーネントに影響
- 7年後、もはや安全に利用できる製品とは言えない





SYNOPSYS®

WindowsのOSアップデートが、高い頻度で実施されているのは経験しているが、
自社用ソフトウェアも含めて、脆弱性はすべてのプログラムに発生しうる

# ソフトウェアのセキュリティ管理

検討課題例

10年前に社員が開発した操業システムのプログラム内で利用されているモジュールに脆弱性が見つかったと報告を受けた。

セキュリティのためのモジュールにも脆弱性は報告されることがある。

- だれが、プログラムの修正をする？
  - その社員の現在の仕事は？
  - 他の人に頼めるプログラム修正？
- モジュールの修正版はいつ入手できるの？
- そのモジュールの修正が、リアルタイム処理に悪影響しないか、テストするには？
- そのモジュールを利用しているプログラムは社内に他にないの？
- たとえ、これを解決できても、また新たな脆弱性が発生する

# ソフトウェアサプライチェーンセキュリティ対策

**米国大統領令（2021年5月）**

- **官民での脅威情報の共有**
- **ソフトウェアサプライチェーンセキュリティ対策の強化**
- **ゼロトラストアーキテクチャへ の移行**

**経済産業省 SBOM(Software Bill of Materials) の普及啓発**

- STEP1：【R3年度実施】 実証(NTT-DATA)を通じたSBOMの効果的な 活用方法の検討
- STEP2：【R4年度実施】 実証の対象拡大による課題整理
  （サプライチェーンにおける共有等）
- STEP3：【R4年度～ 】 制度、ツールの検討・整備 国外との制度調和

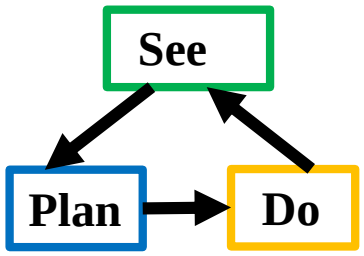
サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースの検討の方向性
経済産業省 商務情報政策局サイバーセキュリティ課 令和3年10月29日より

**SBOMによるソフトウェア資産の管理は、セキュリティとコンプライアンスの解決につながるが、日本ではこれからの段階**

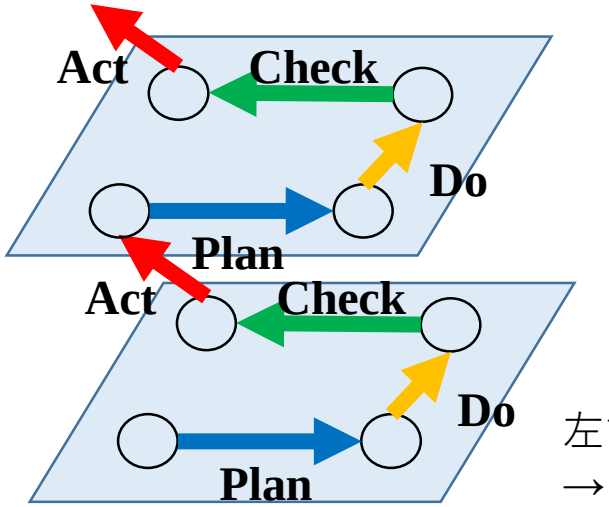
The Linux FoundationによるThe State of Software Bill of Materials（SBOM） and Cybersecurity Readiness(2022)という調査では、回答者の82%がSBOMという言葉を知っており、76%がSBOMニーズに積極的に対応している。
47%の組織が2021年にSBOMを作成または利用しており、78%の組織が2022年にSBOMの作成または利用を予定。

# セキュリティの確保には、運用・保守が重要

- 脆弱性の発生以外にも運用の不備でのインシデントが発生
- サイバーセキュリティ投資を増やせばよいわけでもない。
- **セキュリティツールも保守対象**
- 投資の多寡よりも、つねに見直し、改善するPDCAサイクルを重視すべき
- 確実にスパイラルアップをすすめる組織体制が重要



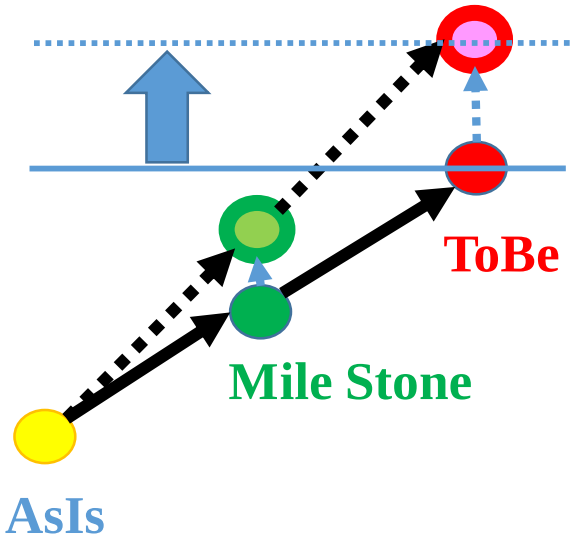

Plan Do See サイクル




左記の〇は状態
→は行動を示す

PDCAによるスパイラルアップ

セキュリティの場合
新たな攻撃が生まれ、
到達目標の見直しが
不可避




計画的成長

# サイバーセキュリティ対策の話題(1)

## サイバーセキュリティのあるべき姿とは？

- どれだけやっても十分になることはない！
  - 常に新たな脅威が現れ、対策の有効性は保持されない。
  - 投資を増やせばセキュリティが向上するわけではない。
    - 運用が大事であり、保守対象が増えると残存脆弱性のリスクは上がる。
- **これだけやっておけばよいというレベルが示されることもない。**
  - **人並みにしておけばインシデントが起こっても許される？**
    - **社会的な許容というのは状況によって変化する**
    - **何が人並み？みんながやっていなければ、自分もやらなくてもいい？**
    - **被害が発生しても、事後の姿勢が評価されて、株価がかえって上昇した例もある**
  - **人並みってガイドラインに従えばいい？**
    - **ガイドラインは着眼点を示しているだけで、それをすればよいというレベルは示されていない。**
    - **そもそもガイドラインは業界のほとんどの業者が実現できることしか書けない！**

# サイバーセキュリティ経営ガイドライン

セキュリティ対策の実施を「**コスト**」と捉えるのではなく、

将来の 事業活動・**成長に必須**なものと位置づけて「**投資**」と捉えることが重要である。

## ＜経営者がリーダーシップをとったセキュリティ対策の推進＞

### （サイバーセキュリティリスクの管理体制構築）

指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定

指示２ サイバーセキュリティリスク管理体制の構築

指示３ サイバーセキュリティ対策のための資源（予算、人材等）確保

### （サイバーセキュリティリスクの特定と対策の実装）

指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

指示５ サイバーセキュリティリスクに対応するための仕組みの構築

**指示６ サイバーセキュリティ対策における PDCA サイクルの実施**（インシデント発生に備えた体制構築）

指示７ インシデント発生時の緊急対応体制の整備

指示８ インシデントによる被害に備えた復旧体制の整備

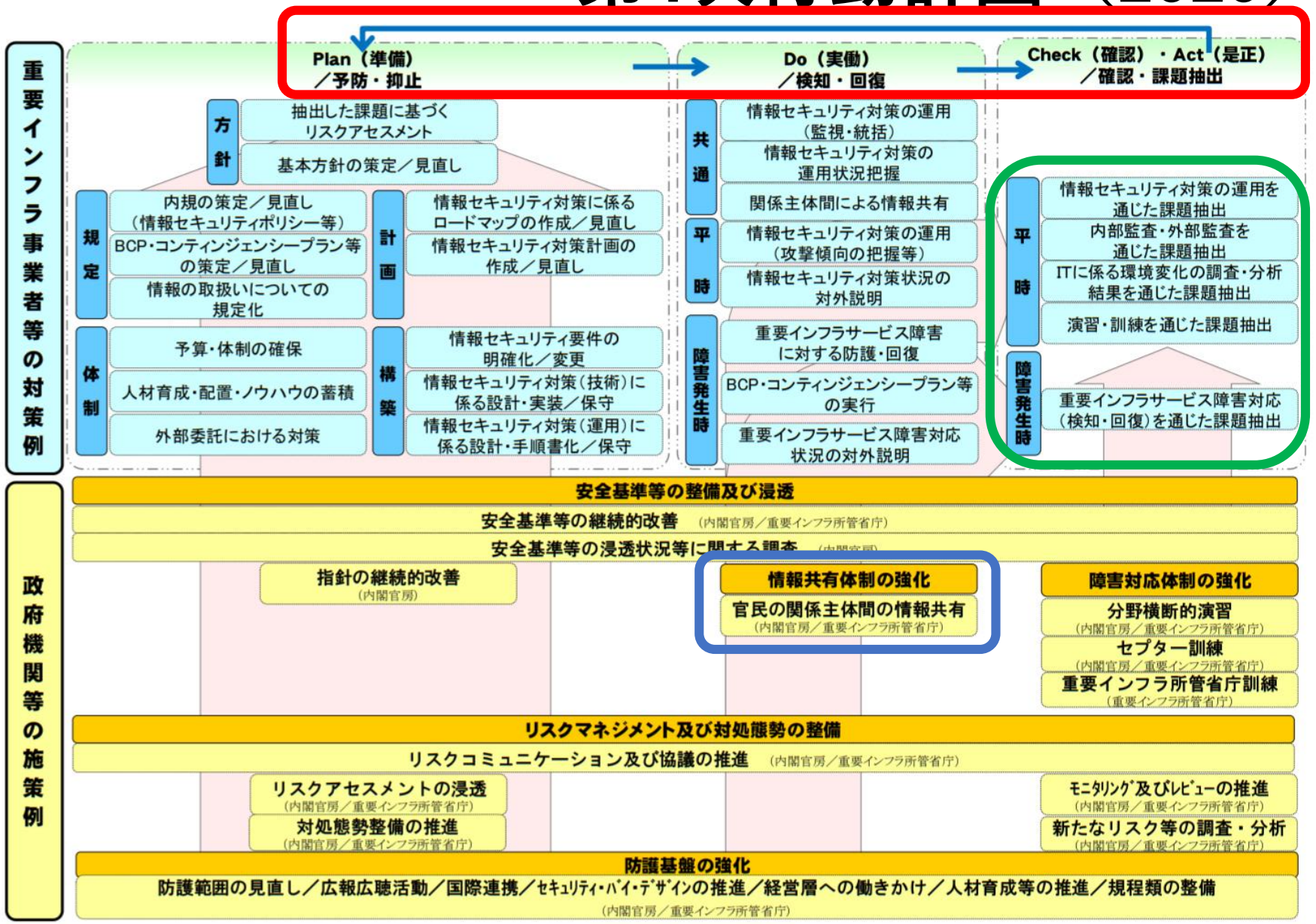
## ＜サプライチェーンセキュリティ対策の推進＞

指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

## ＜ステークホルダーを含めた関係者とのコミュニケーションの推進＞

指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

# 重要インフラの情報セキュリティに係る第4次行動計画（2020）




企業には
**PDCA**サイクルを廻す
体制整備を要求

課題の明示が必要で
課題抽出の活動として
**演習と訓練**が
挙げられている

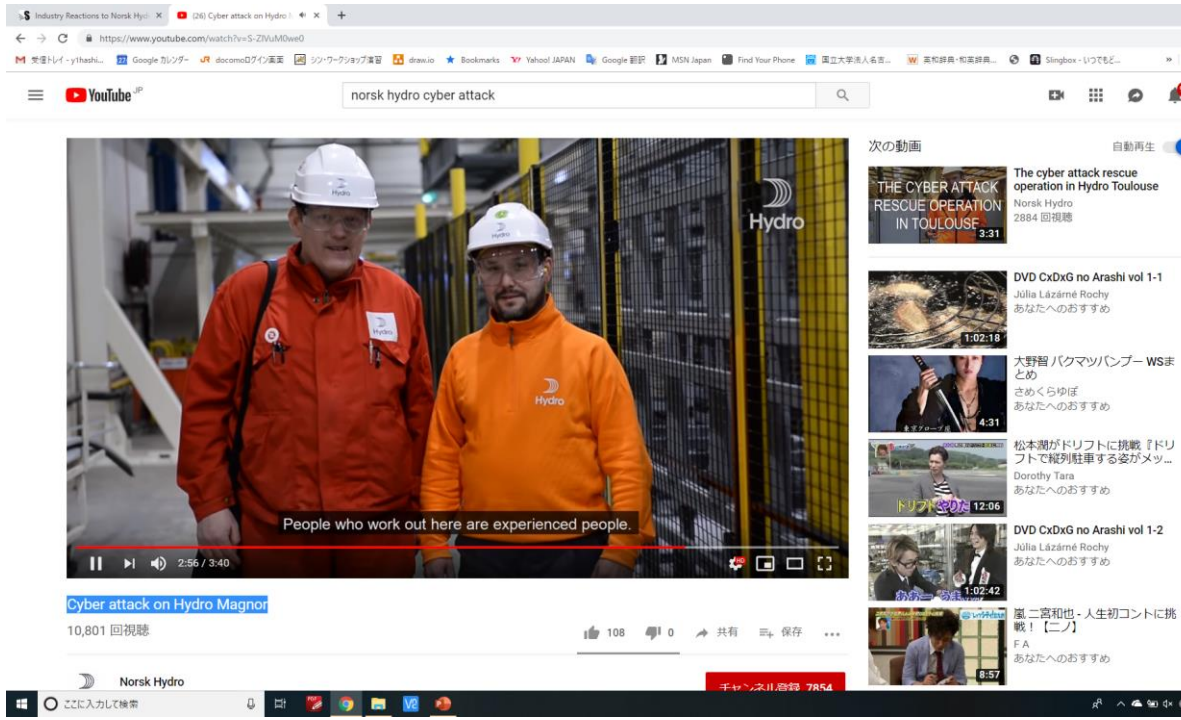
国としては
情報共有を強化したい

# サイバーインシデントが発生しても

- ノルウェーのアルミ製造大手Norsk Hydro
  - 2019年3月19日未明にRansomwareによるサイバー攻撃を受ける。
  - 複数の事業分野に影響
    - $52M in First Quarter
  - **事後対応報告を現場担当者も登場した動画で即座に実施**

    https://www.insurancejournal.com/news/international/2019/04/30/525093.htm

    **事後対応の早さが、高く評価され、株価はかえって上昇**
- 推測
  - ネットワークにハッカーが侵入し、
    その後ネットワーク内で移動して
    「Active Directory」サーバへのアクセス
    - 使われたRansomware 「LockerGoga」
      - 自己伝播機能を持たない
      - 複数のNorsk Hydroの工場に
        同時に被害を与えるために
        アドミン権限を予め取得した攻撃者が
        Active Directoryサーバを使用して同時展開？




https://twitter.com/gossithedog/status/1108287949433651200

# サイバーセキュリティ対策の話題(2)

- **セキュリティへの投資をさぼると、どんなリスクが？**
  - **対策が不十分で事故を起こした責任問題**
    - **本当に事故のリスクは高いのか？サイバー攻撃の現状は？**
  - 市場への参入条件？ セキュアな企業でないと取引できない？
  - これからの時代の市場とは？IoT, Big Data, DXとセキュリティ
    **改善ではなく、革新の時代　新たな価値創造に参画できるか？**

- セキュリティで信頼できる企業と評価されるためには？
  - 製品のセキュリティも重要であるが、企業としての評価も
    - 品質はISO9000, 環境はISO14000,セキュリティはISMS,CSMS?
  - セキュリティ対策にはスパイラルアップを確実に推進する体制の確立が最重要
    - **NIST CSFにある中核組織が存在し、自社のみならず他機関との連携も管理**
  - スパイラルアップのPDCAの要のActを実現推進するには？　監査と演習

# サイバー攻撃の現状調査結果

| No. | 調査機関 | 調査対象 | 内容 |
|---|---|---|---|
| 1 | シーメンスとPonemon-Institute | 中東の石油・ガス事業者 | 担当200人75%が過去1年間に、機密情報の窃取や制御システムの運用障害につながったインシデントが少なくとも1回あった |
| 2 | Corero-NetworkSecurity | 英国の重要インフラ事業者200社 | 過去2件間に70%がサービス障害を経験し、そのうち35%がサイバー攻撃によるものと判明。(17.5%がサイバー攻撃で障害が発生) |
| 3 | Kaspersky-Lab社とPAC社 | 25か国製造、工業、エネルギー、鉱業、運輸、物流の制御システムのCS意思決定者320人 | 31%が過去1年間に1回以上制御システムのサイバーインシデントを経験。 |
| 4 | Fortinet | SCADA/ICSを使用している組織 | 56%が過去1年間にSCADA/ICSに侵入されたことがある |
| 5 | Kaspersky-LabICS-CERT | 同社のセキュリティソリューションが収集 | 41%の組織で制御システムが少なくとも１回攻撃を受けた。トップはインターネットで2位はリムーバブルメディア |
| 6 | Positive-Technologies | 世界各地の石油ガス会社等 | 73%の事業者においてITネットワークへの侵入が可能。ITNWからは82%の事業者でOTへの侵入が可能だった。（合わせると60%がインターネットからOTへ) |

IPA:制御システムの情報セキュリティ ～ 社会インフラや工場に対するサイバー攻撃の脅威と対策(2019)より

# サイバー攻撃を回避できない現状

# マルウェアはすごい勢いで発生している。


コロナ禍で、
さらに、
発生頻度が
上昇している！

2005年から発生したマルウェア種類の積算数

The AV-Test Security Report
https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf

# サイバー攻撃から
# 工場の安全安定操業をどう守るのか？

**拠り所を認識し**
**多重・多層・ゾーン分割で**
**やられても生き残る**

**安全第一で、事業継続も考慮**

# 安全の立場からみたサイバー攻撃の見方

- サイバー攻撃で物理的変化を起こすとしたら、所詮、
  **コントローラの誤動作・誤操作**
- 誤動作・誤操作を考慮しない安全解析はありえない。
- 安全解析で想定した事態以外の事故は起こりえない。
- サイバー攻撃で、甚大な事故が発生するとしたら、
  安全対策が有効に働かない事態
- **サーモスタットやリレーの緊急遮断、安全弁等**

  **ソフトウェアに依存しない対策は攻略されない**
- **わざと全停電にして、フェイルセーフに任せたら、
  サイバー攻撃下でも、安全に停止できるはず。**
- でも、そのような処置が必要な状態と**気づけなかったら危ない**
- **想定外のサイバー攻撃にも有効な、拠り所はないか？**
- **拠り所を広げていく取り組みもあるのでは**

# コントローラは指示通り動くのが仕様

## 製造現場には、サイバーリスクがいっぱい！

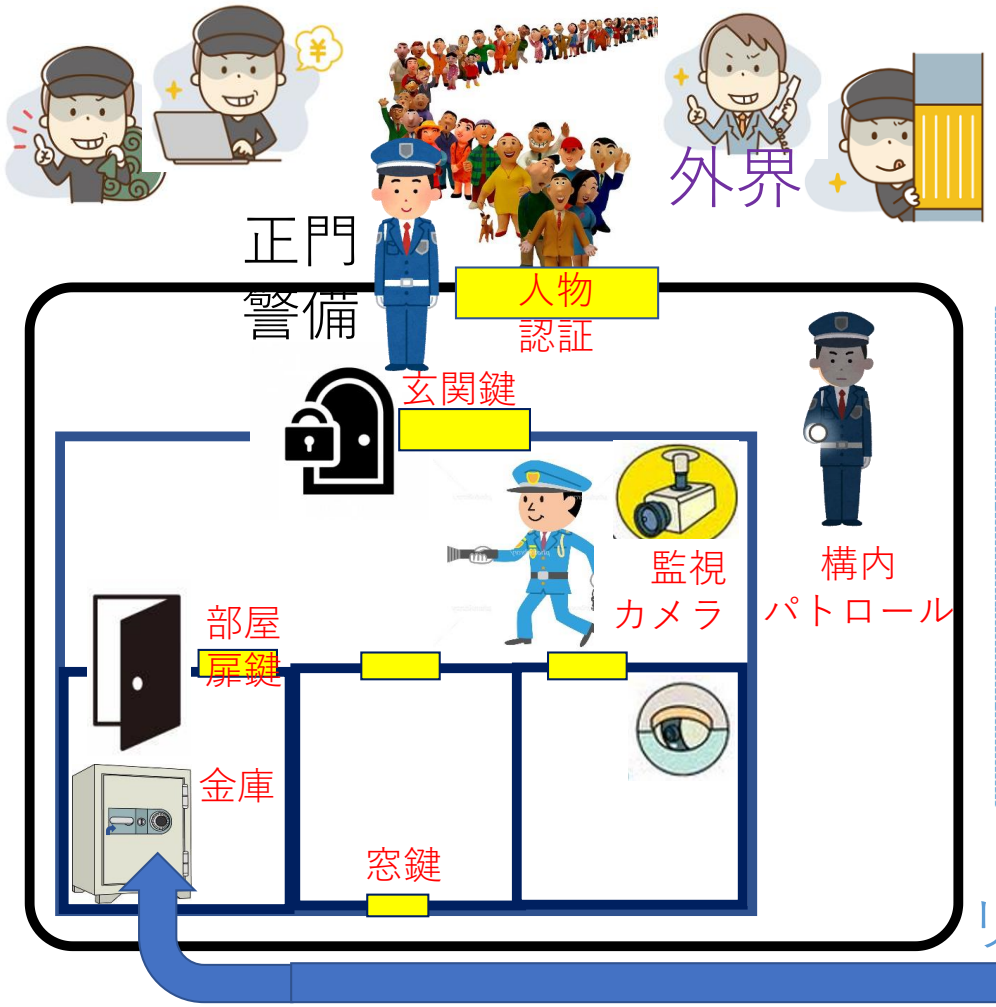

ＤＣＳに侵入しなくても
リモコンを攻略できれば
アクシデントを発生可能

保守PCを
ウィルスチェックしても、
検出は2,3割に過ぎない

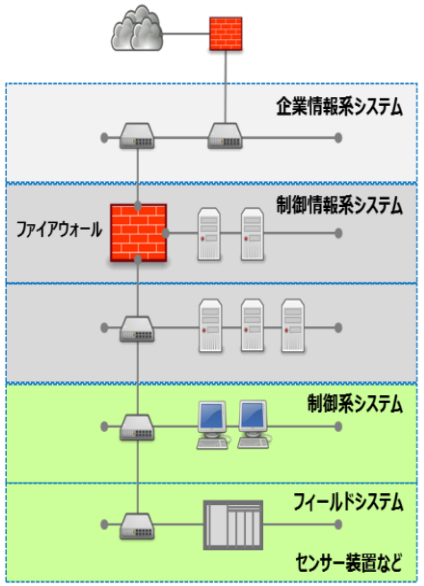
保守の管理は
ちゃんと動くかで
指定以外の
動きをしないという
チェックはしない

# セキュリティの深層防護と安全の独立防護層

## 深層防護とTrusted Networks




Zone & Conduitで
(エリア)と(通路)
セキュリティレベルを
検討

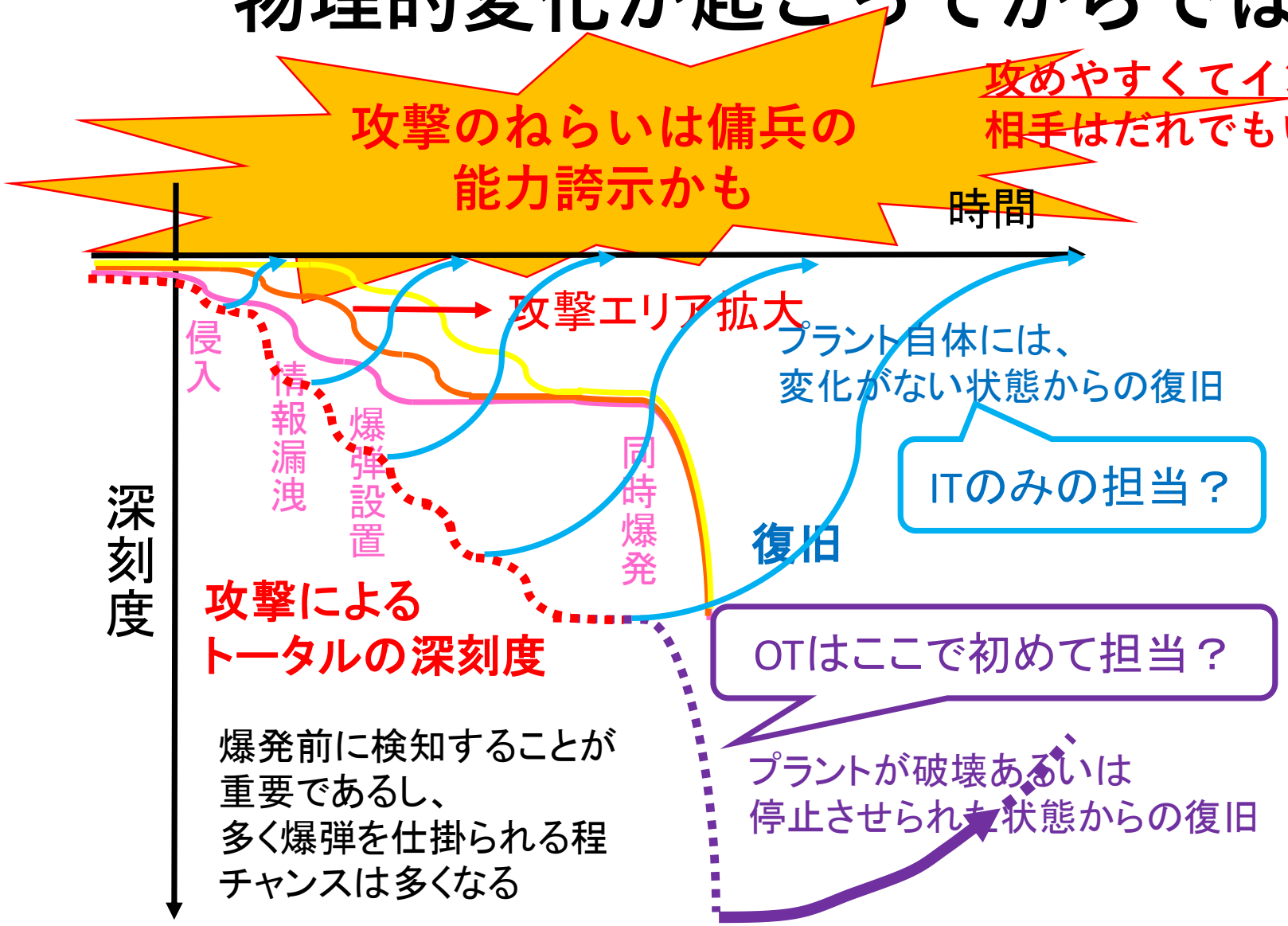




⇐VIII 通報不稼働
⇐VII 通報不稼働等

⇐IV 不稼働
⇐III 不稼働
⇐II 改竄・隠蔽

# 物理的変化が起こってからでは遅い！




現在のほとんどの
操業現場では、
物理的変化を
見つけるセンサ類は
あるが、
制御ネットワークを
監視してる例は
ほとんどない。

見つけたときには
遅いというリスクを
意識して、
ネットワーク内の
監視を強化すべき

**複数個所で同時に被害を発生させることで、被害が甚大になる**
**（救急車も消防車も間に合わない）被害が発生する前になんとか**

# サイバーセキュリティ対策の話題(2)

- **セキュリティへの投資をさぼると、どんなリスクが？**
  - 対策が不十分で事故を起こした責任問題
    - 本当に事故のリスクは高いのか？サイバー攻撃の現状は？
  - **市場への参入条件？ セキュアな企業でないと取引できない？**
    - **サプラインチェーンリスク（中国製の部品は×？）、商品にはトレーサビリティの情報も必要**
  - **これからの時代の市場とは？IoT, Big Data, DXとセキュリティ**
    **改善ではなく、革新の時代　新たな価値創造に参画できるか？**

- セキュリティで信頼できる企業と評価されるためには？
  - 製品のセキュリティも重要であるが、企業としての評価も
    - 品質はISO9000, 環境はISO14000,セキュリティはISMS,CSMS??
  - セキュリティ対策にはスパイラルアップを確実に推進する体制の確立が最重要
    - **NIST CSFにある中核組織が存在し、自社のみならず他機関との連携も管理**
  - スパイラルアップのPDCAの要のActを実現推進するには？　監査と演習
  - **企業内演習・教育の提案**

# セキュアな企業でないと取引できない？

- Green取引では、鉛の使用が一切禁止され、装置の設計にも影響した
- 中国製部品から不審な発信があったと、中国製部品が入っていると米国に輸出できなくなった。
- ソフトウェアも変な機能が忍ばされていないか管理する必要があり、SBOMの管理がされていないと、市場に参入できなくなる？
- テストも仕様の動きをするだけでなく、仕様以外の挙動をしないことが要求されるようになる？
- 製品やサービスで脆弱性が発生したらいち早く対策パッチを供給するし、パッチ前の対策に対応するようなセキュリティ対策がないと、購入してもらえない？
- 製品とともに提供されるトレーサビリティの情報にもセキュリティは不可欠
- 製品やサービスではなく、企業としての信用が取引の可否に影響する？

# これからの時代への投資としてのセキュリティ？

- 革新による新たな価値創造の時代
- IoT,AI, Big Data, 3Dプリンタに期待される革新とセキュリティ
- まず、IoT(Internet of Things)の革新性、次に、AIとBig Dataの革新性をSoS(System of Systems)という観点で述べ、そこへのセキュリティの必要性について考察する。
- IoTは共通基盤のインターネットにモノをつなげること
- AIは人間の目や認識の機能を持ち、大量のデータを処理できるもの
- Big DataとDXは、様々な業務のデータが知識構造に従って整理すること
- クラウドは豊かな計算機資源があり、内部のサーバは柔軟に切り替わりながら更新され、サービスを継続する。クラウド内の様々なインテリジェンスが自由に組み合わせ、新たなサービスを容易に実現できる。

# 革新の時代とは？

例）iPhoneのSiriは
つながって作動

⓪ 手動、風力、馬車

① 蒸気機関による大量生産運輸　産業革命

② 電動（コンパクト、強力、コントロール容易）

③ プログラム（マイコン制御、オートメーション）

**モノにインテリジェントが載る**

**④ IoT(Internet of Things), Cloud, SOS(System of Systems)**

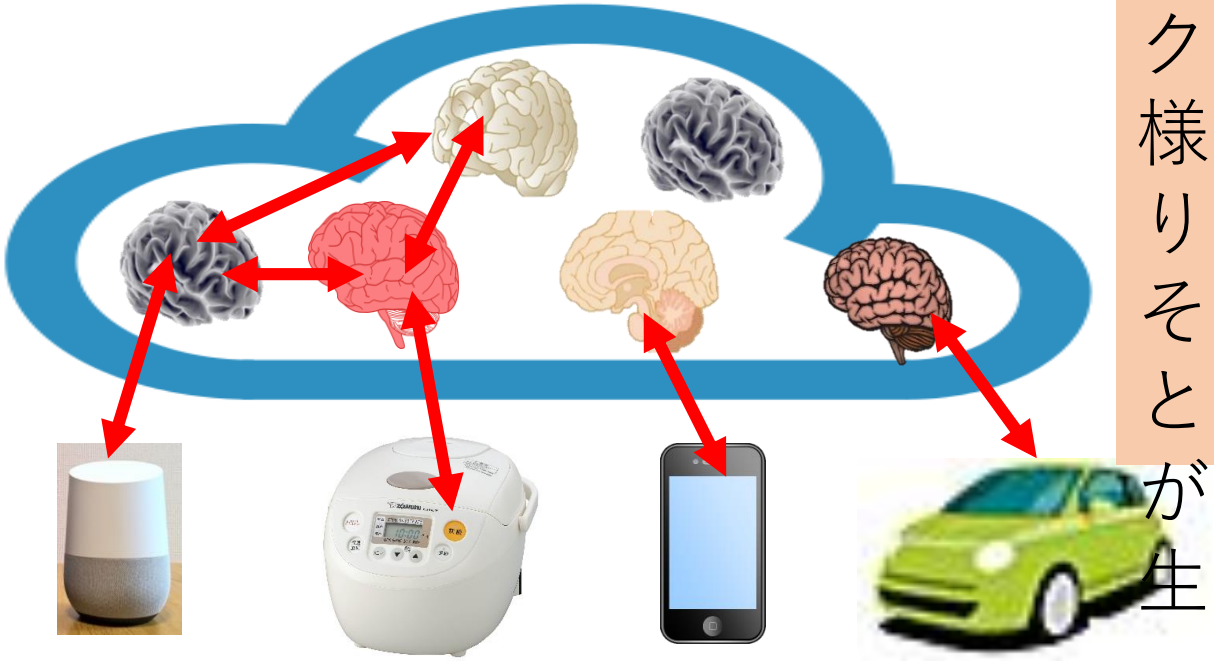
④って
何？

**モノからインテリジェントが離れる　つながることに革新性**





# Cloudでは知能がつながって新たな知能が



クラウドには、
様々な情報が集まり、
それらをつなげると、新たなサービスが
生まれる

## Google Mapの渋滞情報

- Google mapのユーザーは今いる場所の地図を得たいし、経路もナビしてほしいからGPS情報をGoogleに送る
- Googleは膨大に集まるGPS情報から
車の移動を推算し、地図上に表示

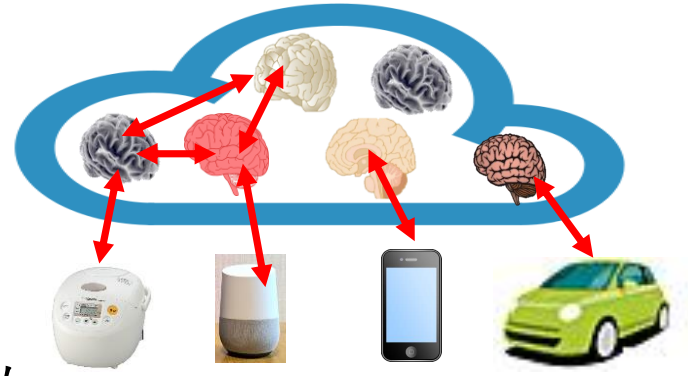
# IoTの革新性

**インテリジェンスがモノから離れてクラウドへ**

- **物理的** (CPU, Memory, HDD, etc.)
- **空間的** (Access to all over the world)
- **時間的** (Past, Present, Predicted Future)

**拘束から解放される**

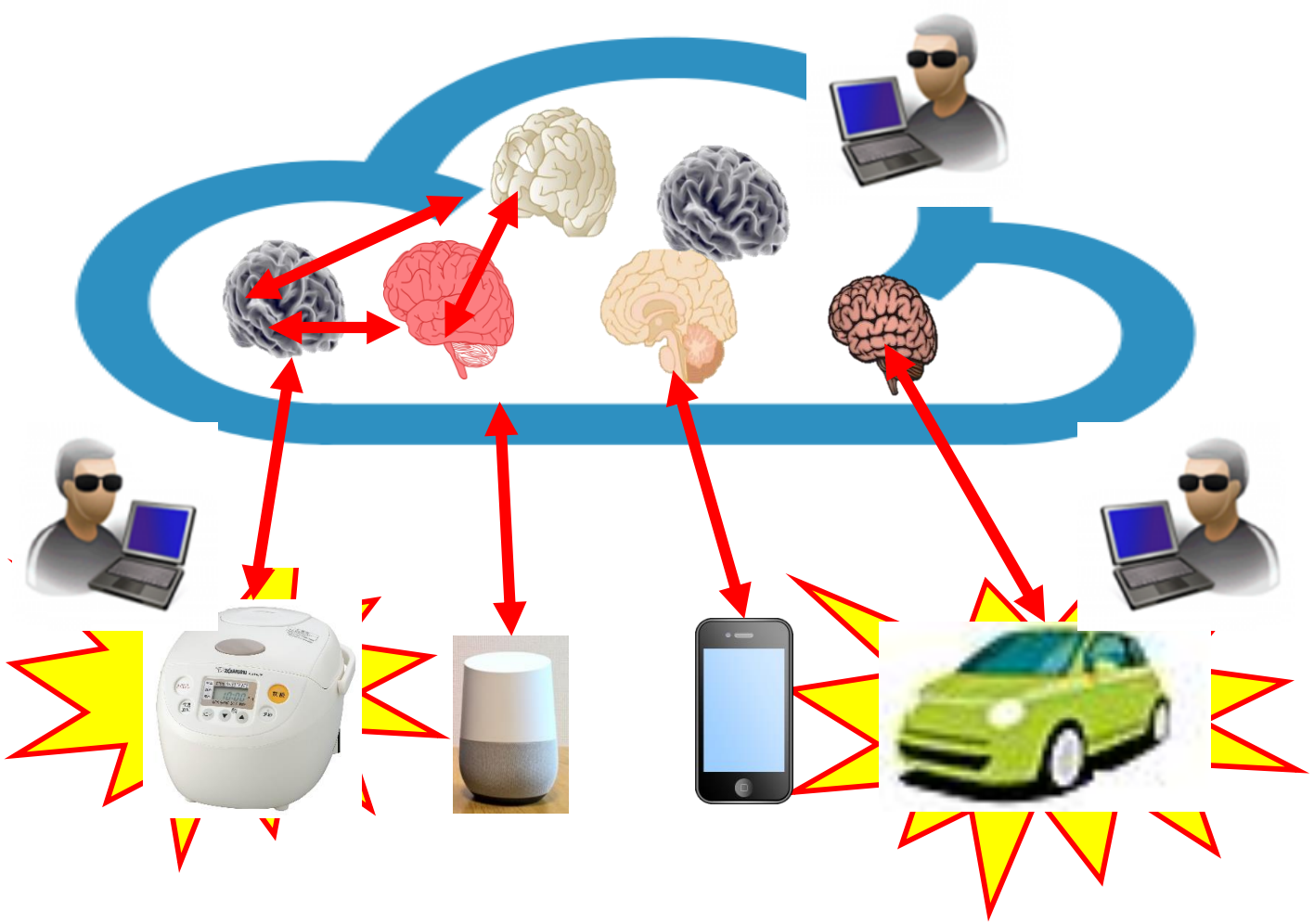
**Innovation**



**System:** 特定の**目的**で開発

**System of Systems**: 開発時にはなかった
**新たな機能**を連動して発揮

# 革新にはセキュリティが不可欠



**“Things” がCloud内の知能に従うと、**

**サイバー攻撃で危険な状況が簡単に生じる！**

# 制御システムのセキュリティ対策の方向性

制御システムのサイバーセキュリティ対策は、以下の特性に注目し、

- インテリジェントは脆弱性の源
- 脆弱性は常に発生し、セキュリティ対策にはきりがない
- セキュリティパッチはすぐに適用したい

プラントというモノを扱う制御システムを考慮すると、

- フィールドに固定されるものは、シンプルなインテリジェントに限る
- いかにシンプルでも、パッチを充てられる余裕は与える
- インテリジェントは、柔軟なセキュリティ対策ができるところに置く
- 通信遮断での機能不全が危惧されるインテリジェントは、バックアップやアップデートが容易な環境をフィールドに置くが、保守を考慮してできるだけシンプルにする
- リアルタイムの通信が必然でないインテリジェンスはクラウドに置く

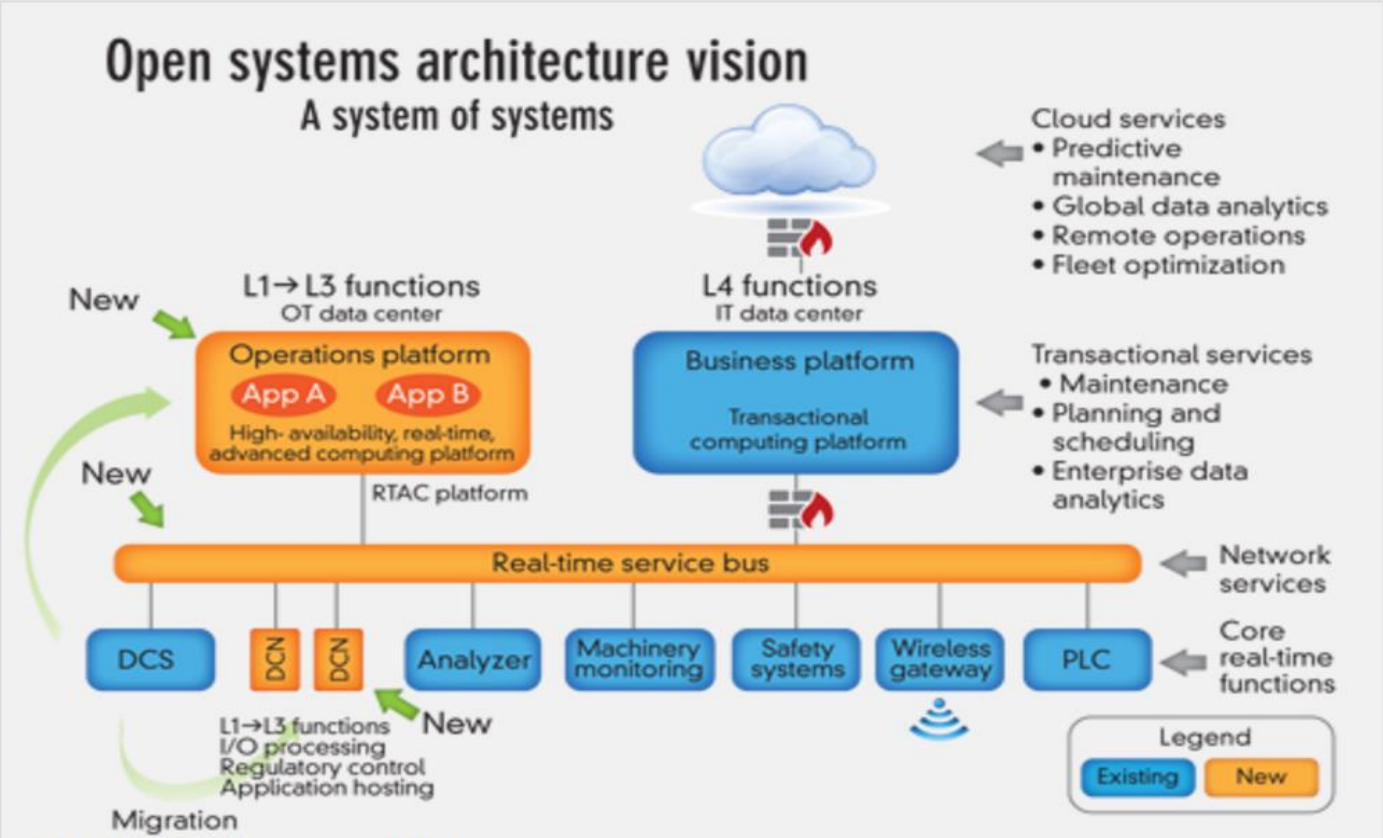
# 安価にスマート化をしていいの？

- ラズベリーパイ　ゼロは、5ドルPCとして開発され、HDMIでテレビに接続し、キーボードとマウスをUSBで接続すれば、本格的なPCになる。
- 無線デバイスをWEB サーバーにして、世界のどこからでも情報をとれるようにしても、500円でできる。

- IoTって、安価なスマート機器をばらまくこと？
- スマートバルブ、スマートセンサー、・・・
  どんどんスマート化はできるだろうけど。
- **それって、本当にありがたいこと？**
- 限られたCPU能力、メモリでなんとか実現できている状態で、脆弱性がみつかったら？
- パッチをあてられず、買いなおすことになる？
- **結局、ゴミになるか、セキュリティホールになるか**

# ExxonMobil次世代生産システム

Lockeed Martinと2016年1月14日にnext-generation, open and secure automation system for process industriesの開発のSystem Integratorとして契約




**DCS dream taking flight**

ExxonMobil envisions a new "system of systems" that will allow it to more easily adapt its operations environment to change needs and opportunities. Graphic by ExxonMobil.

Lockeed Martin: Future Airborne Capability Environment (FACE) Consortium since 2010

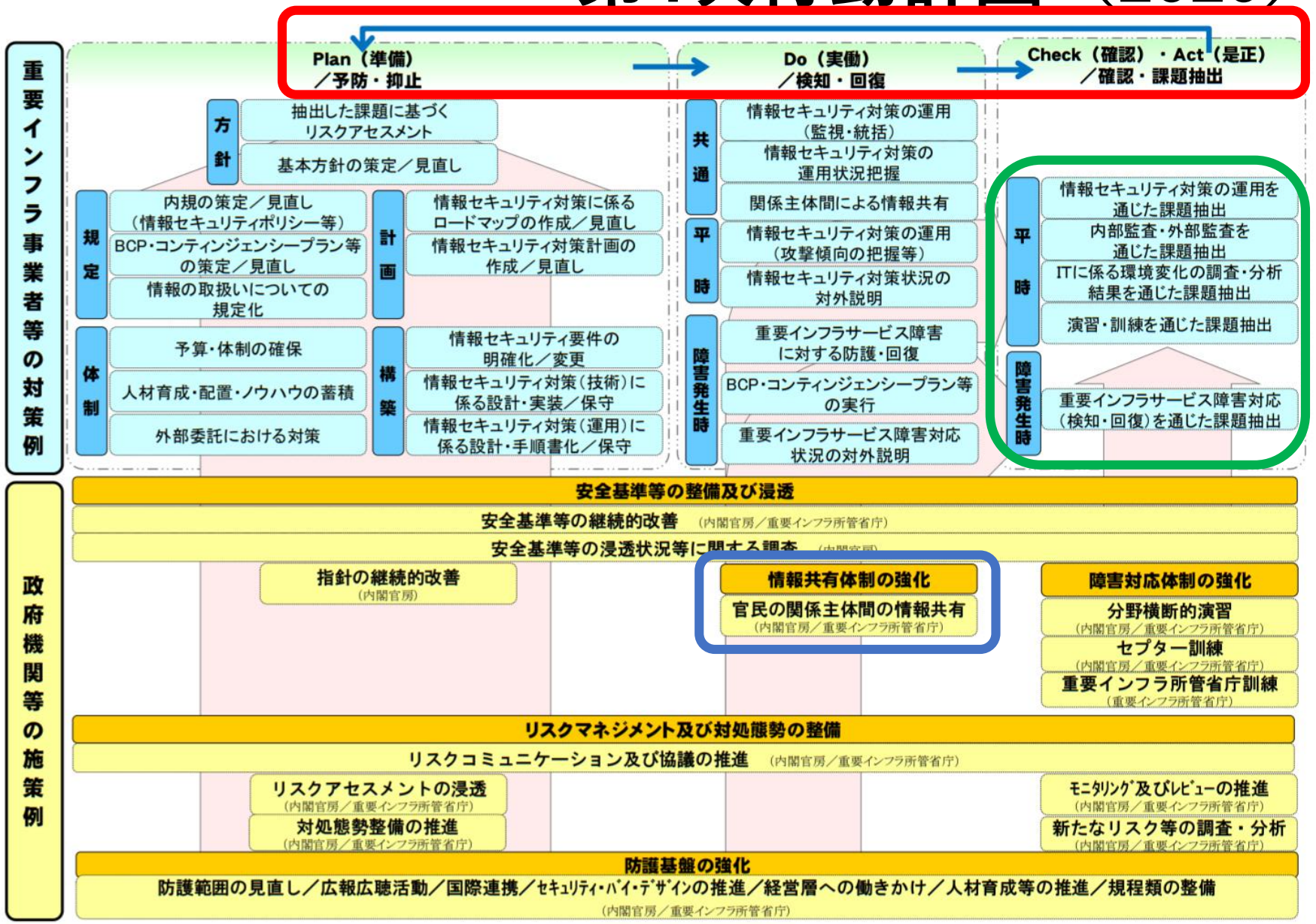
# サイバーセキュリティ対策の話題(2)

- **セキュリティへの投資をさぼると、どんなリスクが？**
  - 対策が不十分で事故を起こした責任問題
    - 本当に事故のリスクは高いのか？サイバー攻撃の現状は？
  - 市場への参入条件？ セキュアな企業でないと取引できない？
    - サプラインチェーンリスク（中国製の部品は×？）、商品にはトレーサビリティの情報も必要
  - これからの時代の市場とは？IoT, Big Data, DXとセキュリティ

    **改善ではなく、革新の時代　新たな価値創造に参画できるか？**

- **セキュリティで信頼できる企業と評価されるためには？**
  - 製品のセキュリティも重要であるが、企業としての評価も
    - 品質はISO9000, 環境はISO14000,セキュリティはISMS,CSMS??
  - セキュリティ対策にはスパイラルアップを確実に推進する体制の確立が最重要
    - **NIST CSFにある中核組織が存在し、自社のみならず他機関との連携も管理**
  - スパイラルアップのPDCAの要のActを実現推進するには？　監査と演習
  - **企業内演習・教育の提案**

# 重要インフラの情報セキュリティに係る第4次行動計画（2020）

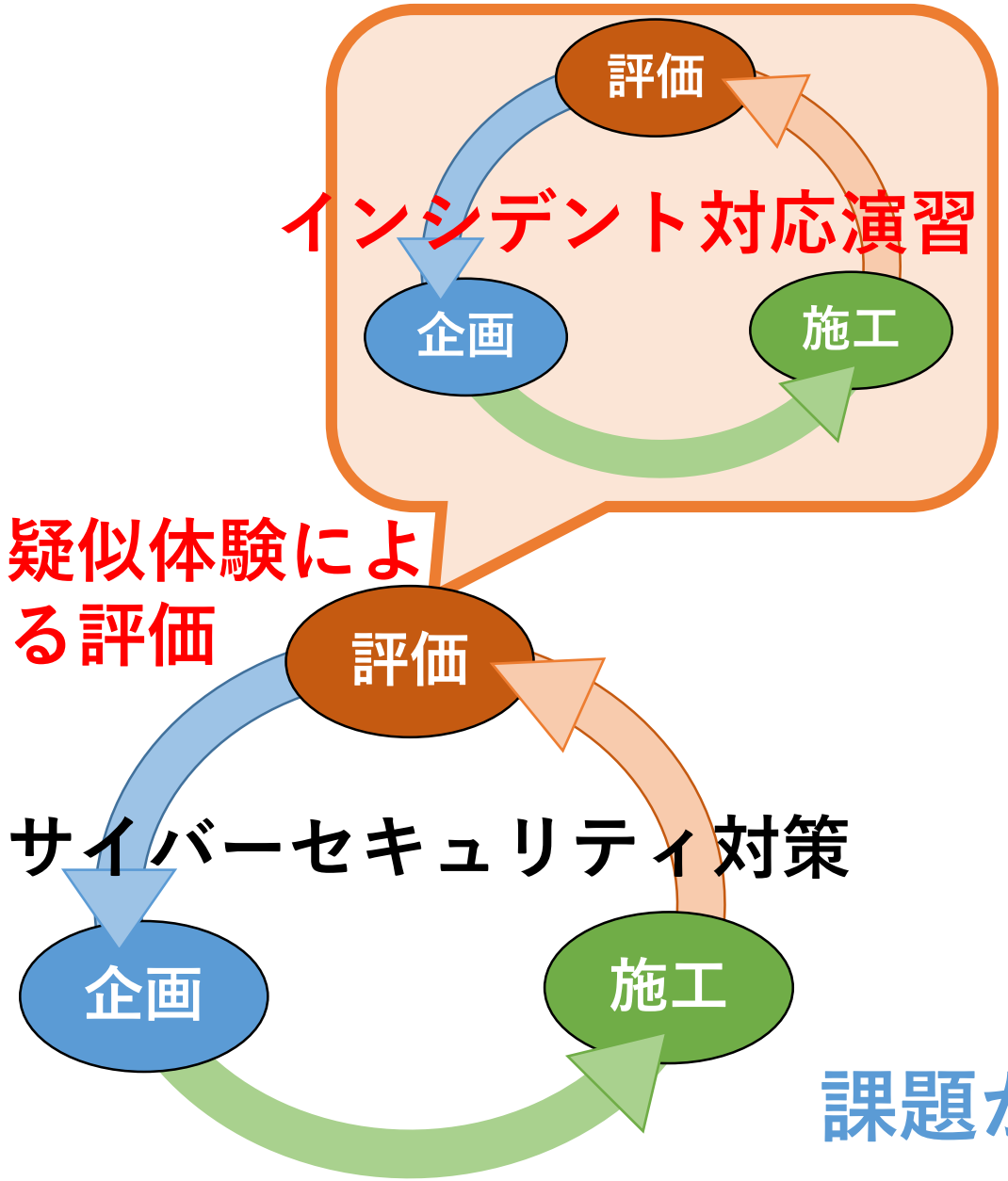



企業には
**PDCA**サイクルを廻す
体制整備を要求

課題の明示が必要で
課題抽出の活動として
**演習と訓練**が
挙げられている

国としては
情報共有を強化したい

# サイバーインシデント演習への期待




- **想定外が不可避なサイバーセキュリティにはレジリエンスが重要**
- **レジリエンス**には、非常時を想像する能力が必要。
- **想像力**向上には**疑似体験を繰り返すこと**が有用
- サイバーセキュリティ対策の**評価**には**疑似体験**が不可欠
- **セキュリティをスパイラルアップ**させるPDCAサイクルの原動力として、インシデント対応演習が有用
- 演習により**次の課題**を明確にする

**課題が抽出できてこそ、演習の価値がある。**

# いざ、事故が発生したら、危険なのは操業現場

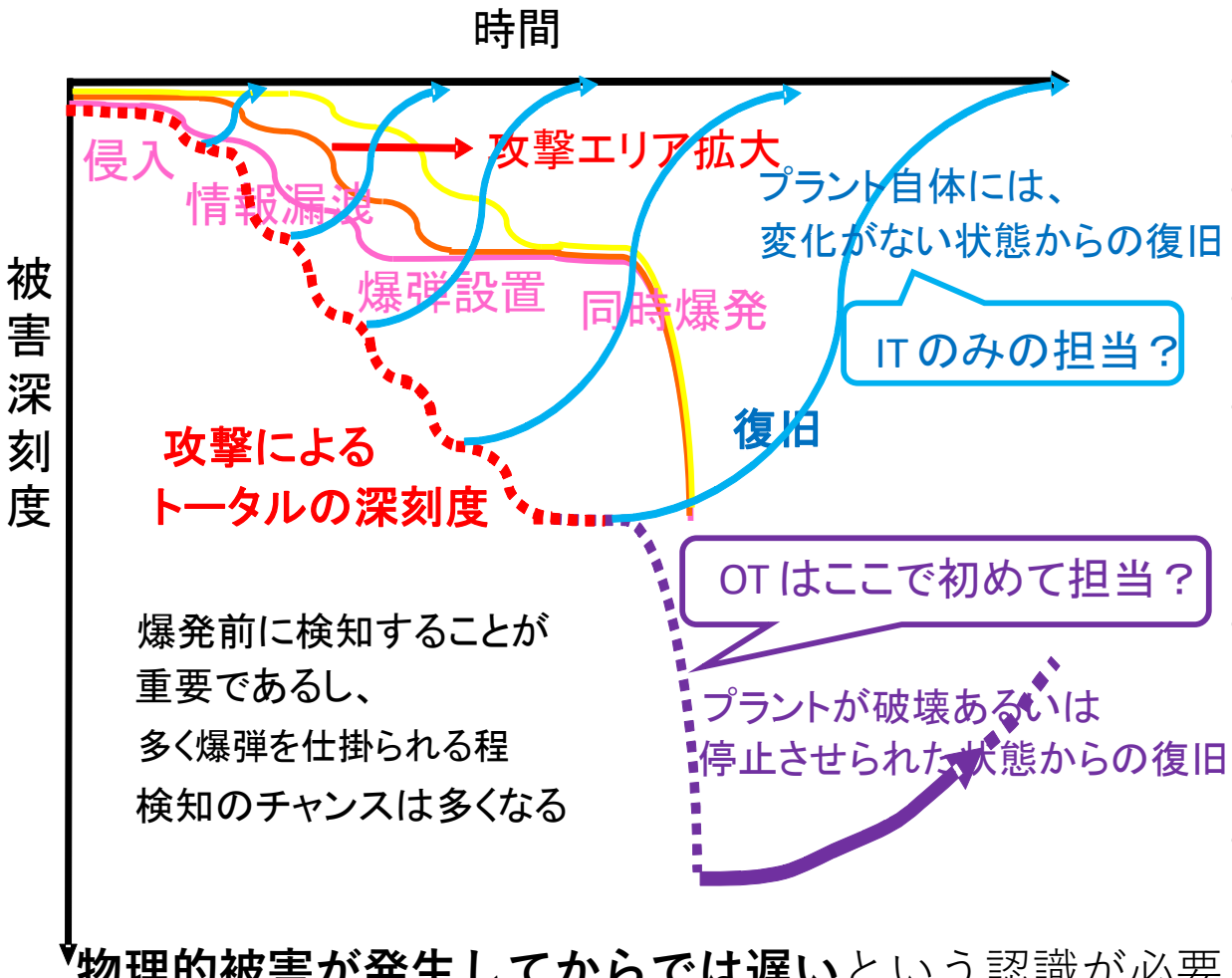
- サイバー攻撃も安全破綻の原因の一つである。
- まず、**安全第一**でサイバー攻撃への対策を考えよう。
- **サイバー攻撃が従来の安全の対象と異なる**重要な点は**どんどん新しいものが生まれ、きりがない**こと。
- **イタチごっこ**なら取り組みたくないともいえない。
- 「**想定外だったから、しかたがない**」と人が死ぬ事故が発生してもいえるか？
- 安全は最優先だが、**事業継続**の観点も必要

**サイバー攻撃のリスクって？**

十分

- **想定外は不可避であり、システムでは対応しきれない。**
- **安全ではSafety-I(事故を起こさない能力)から**
  **Safety-II(被害に対応する能力)が重要視**
  **人が危険源からヒーローへ**
- **組織の対応能力（レジリエンス）の向上には？**

# 操業現場の技術者にとっての制御システムセキュリティ




**物理的被害が発生してからでは遅い**という認識が必要

**サイバー攻撃からの被害防止に対して、**
**自分が行動すべきことは何と考える姿勢を**
**演習をきっかけにもってほしい**

- 物理的変化が起これば、**最も危険にさらされる立場**である。
- サイバーセキュリティの勉強よりも**リスクの理解が大事**
- 監視画面では変化を検知できないまま、プラントで甚大事故が発生させるサイバー攻撃もありうることを意識すべき
- サイバー攻撃は対処が遅れると、その間に被害が拡大するので早期対応が必要だが、そのための**操業現場の貢献とは？**
- 生産指示やトレーサビリティのための実績報告などに通信は必要だが、**通信の代替手段を確保**できていれば、通信遮断の判断が容易になり、**サイバー攻撃が確信できない段階での早期対応**が可能になる。
- 高度制御や運転支援、データサーバーなどへのサイバー攻撃が疑われるとき、**それらがなくても操業できる**と現場が対応できれば、早期の隔離が可能になり、被害拡大を防止できる。
- コントローラの隔離は困難なので、**コントローラが信頼できない状況**ではすぐ**プラント停止**すべきか、**現場を監視しながら操業継続**できるのか、リスク評価とともに早く判断できるように**事前に検討**しておきたい。
- 保守作業などで、感染が持ち込まれたり、発信機が取り付けられるリスクがあることも意識すべき。**作業監視**の責任は操業現場にもあるのでは。

# 制御システムセキュリティ向上演習
# IMANE(Incident MANagement Exercise)

戦略的イノベーション創造プログラム(SIP)において、セキュリティ人材育成のテーマを担当し、IMANEシリーズを開発（2014～2018）

## (EX-1) IMANE-DEMO

携帯できるシステムで、制御系でのサイバー攻撃を体験

- まず、他人事ではない問題だと意識してもらう
  現場の人を、サイバーインシデント対応演習に引き込むのに有用

## (EX-2) IMANE-CARD

CARDを並べるグループワークで、インシデント時に求められる組織間連係をイメージする演習

- 事前準備ではなく、演習参加により、自分の部署の役割と必要な連絡を意識してもらうことで、
  演習導入を容易にする演習形態

## (EX-3) IMANE-PC

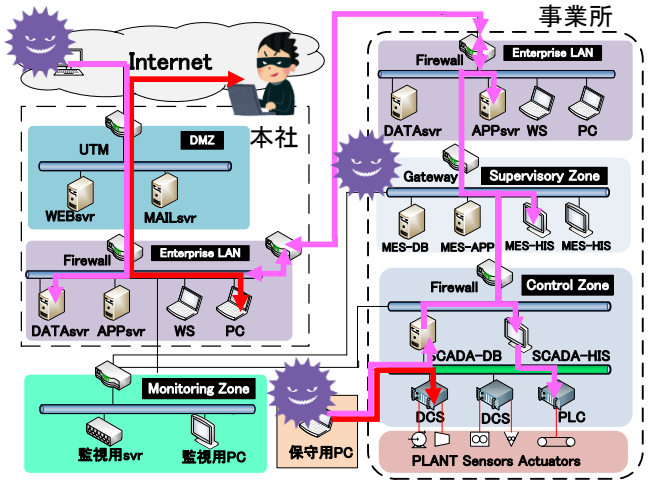
PCを用いてインシデント発生時の組織間連携を疑似体験する演習

- 実施上の問題を洗い出すために、振り返りを重視し、PDCAを推進するツールとするため、異なるシナリオでの演習をデータ入替で実現し、実施結果をデータ化し、比較を容易にする演習形態

**現在も演習の開発や改良をつづけています（ぜひ演習をいっしょに検討しましょう）**

# IMANE-DEMO(1)

- 工業計装の機器で構築した制御系をKali Linuxで自分で攻撃
- 攻撃されている状況での通信を監視し、
  検知できるとした場合の防御について考える




制御ネットワークに侵入できれば
SCADA, Local Controllerを
操作するだけでなく、
気づけない攻撃が実現できること
および通信監視で攻撃が見えること
を理解する

SCADA

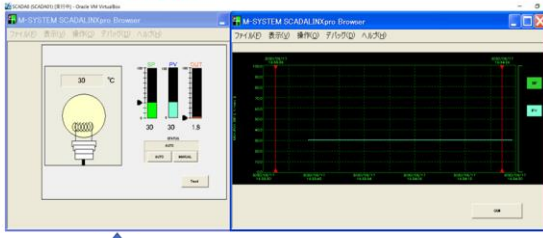
通信

Local Controller

センサー
アクチュエータ

Plant

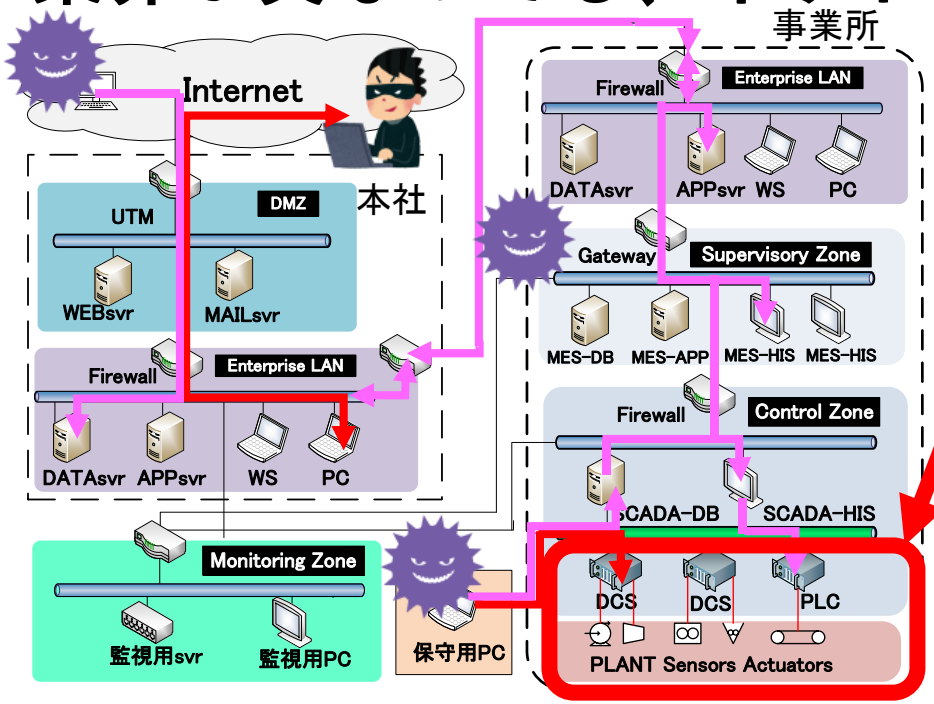

ほぼマウス操作だけで
様々な攻撃を繰り広げる
ことが可能


監視画面は変化しないのに
プラントは危険な状態になる
攻撃も可能

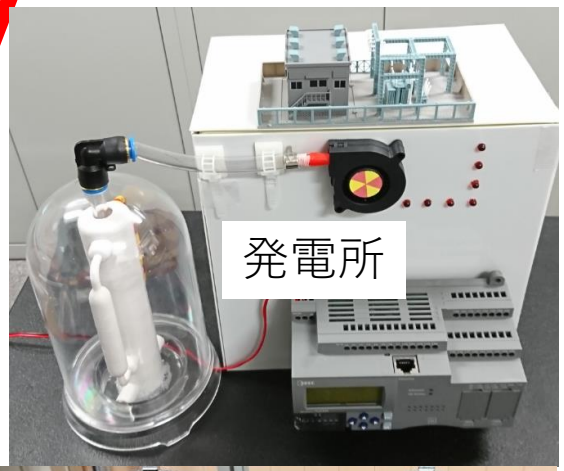
# IMANE-DEMO(2)

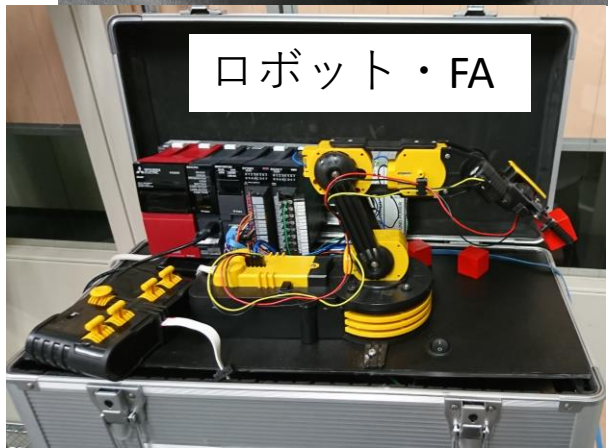
## 業界が異なっても、ネットワーク構造は共通




デモシステムは、プラント部分を入れ替えるだけで、ほぼ共通で構築可能





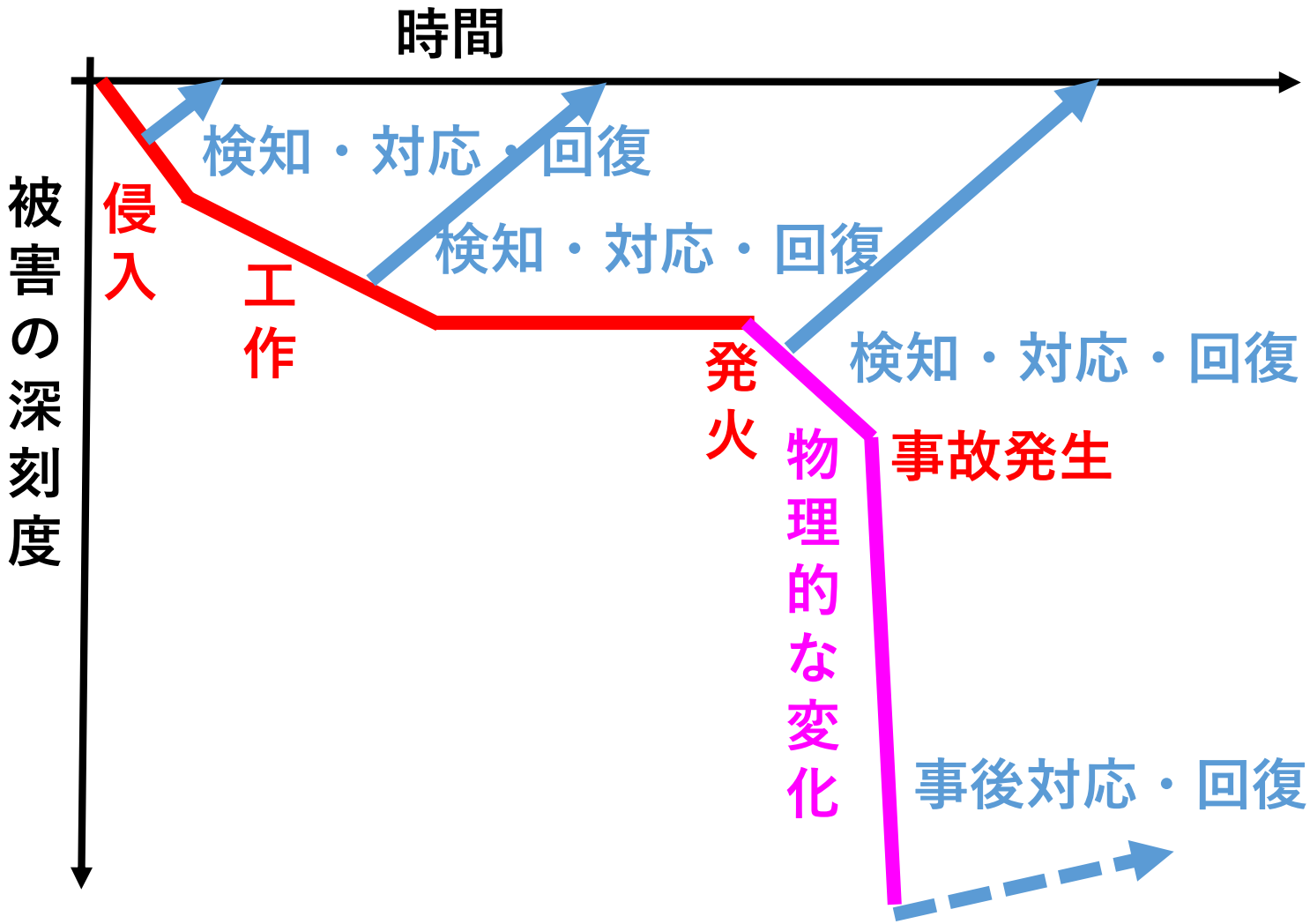




## 様々なシナリオを実施可能

- フィッシングサイトによる企業内LANへの侵入
- 管理者権限獲得
- 踏み台設置による侵入進展
- 通信監視によるパスワード搾取
- 攻撃ツールの送り込み
- 隠蔽工作
- コントローラの不正操作
- 通信妨害（DOS攻撃）

# IMANE-X （New!!）

サイバー攻撃の進展を**侵入、工作、発火、事故発生**という4段階に整理し、**各段階での対応**を議論する。




多重な攻撃が**同時発火**して
救急車も消防車も足らない
甚大な事故になる可能性

**物理的に変化したときには、遅すぎる**と認識すべき

**早期対応**が望まれるが、
その**可能性を演習で議論**

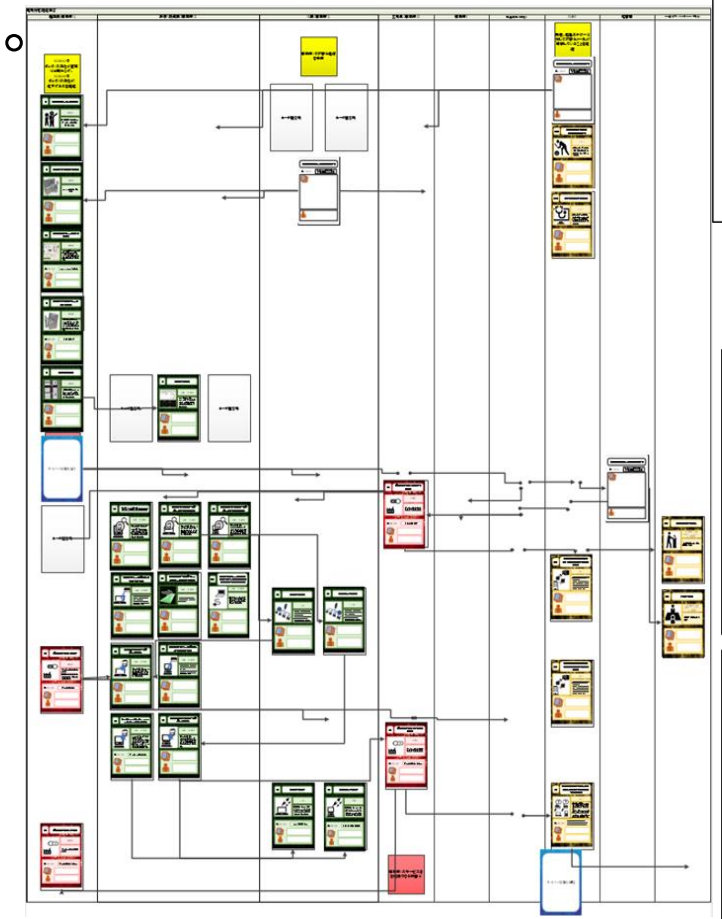
**部門間の課題認識の共有**を
演習で実現したい

# IMANE-CARD

- 演習対象のインシデント対応の流れをカードを並べながら議論
- カードを正しく配置できるかではなく、
  インシデント発生時の状況をイメージし、
  各部署の対応の連携での現状の課題を抽出。

対応部署

時間経過





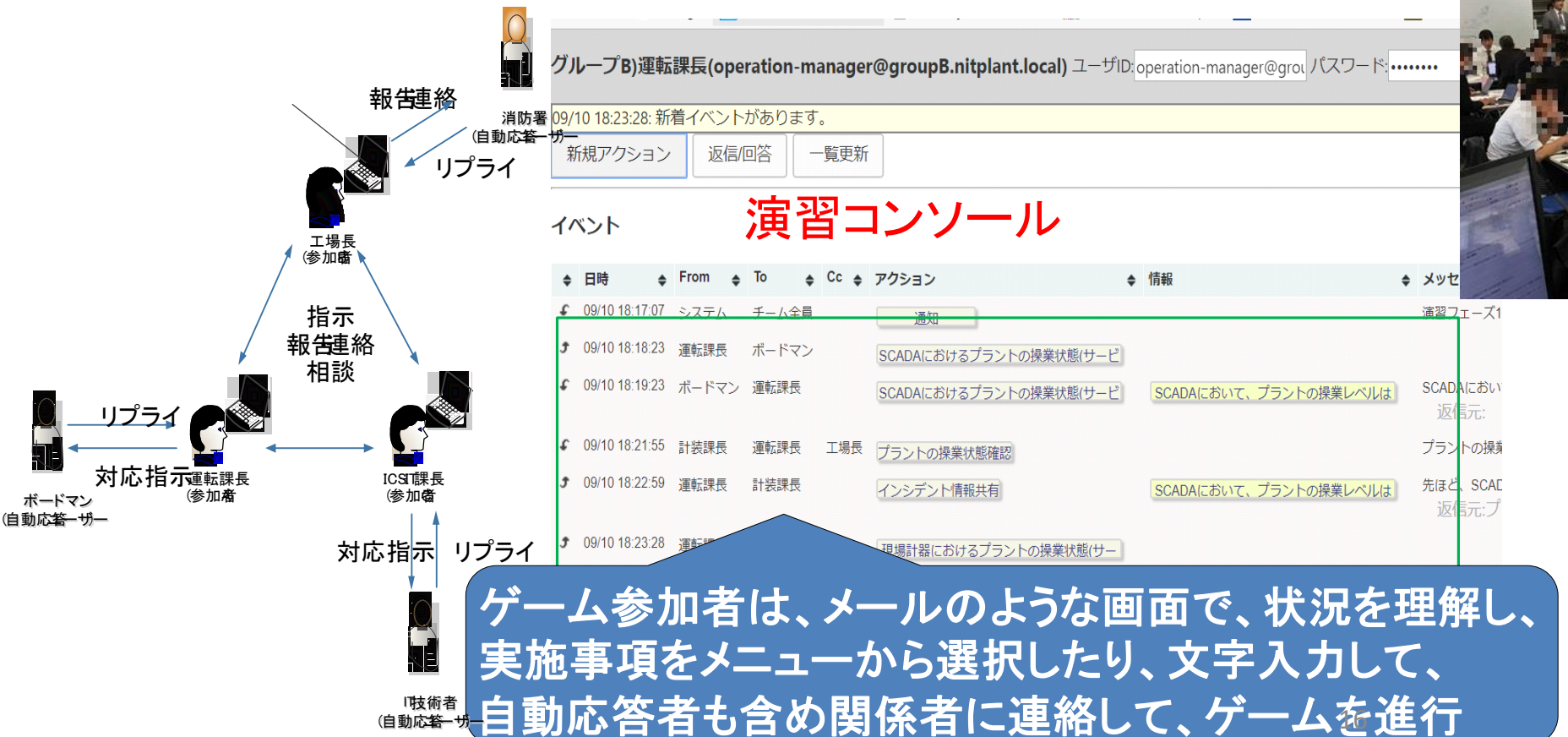
アクションカード


リスクカード

**演習は決まった手順の確認が目的ではなく、**
**演習で課題を抽出することでPDCAを推進する。**

# IMANE-PC

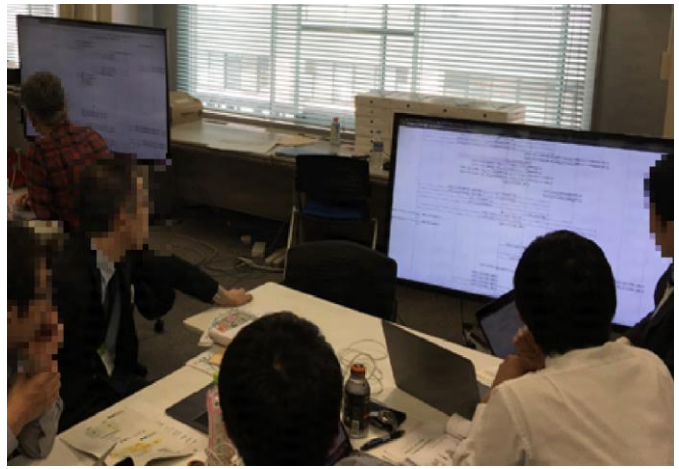
- コンピュータを利用した演習




ゲーム参加者は、メールのような画面で、状況を理解し、
実施事項をメニューから選択したり、文字入力して、
自動応答者も含め関係者に連絡して、ゲームを進行

演習実施風景

演習直後に振り返り



ヒューマンインターフェイスはシンプルだが、
だからこそ様々な事業所のシナリオに対応しやすく、演習実施頻度を高くしやすい。
課題抽出に重要な振り返りが直後に実施できる。