SY-76 [安全部会シンポジウム]
スマートファクトリーと安全
総合討論

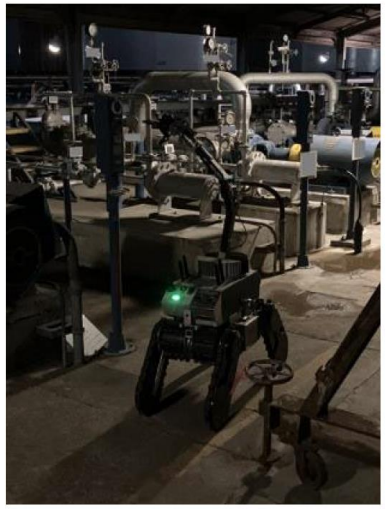
司会：名工大 橋本芳宏

化学工学会第55回秋季大会　2024年9月12日(木)北海道大学において

SCEJ 公益社団法人 化学工学会

スマート保安に関する変革要素（人材不足）

- **防爆ロボット　ドローンで空中から、ロボットで地上から**

普及させて、可能性を向上させよう。

- **生成AI　道具というより、優秀人材として活用すべき**
  - 人間より有能で、いやがらずに、どこまでも付き合ってくれる。
  - PFDを画像で与えて、物質情報、操業条件を与えたら HAZOP Studyすらやってくれる。

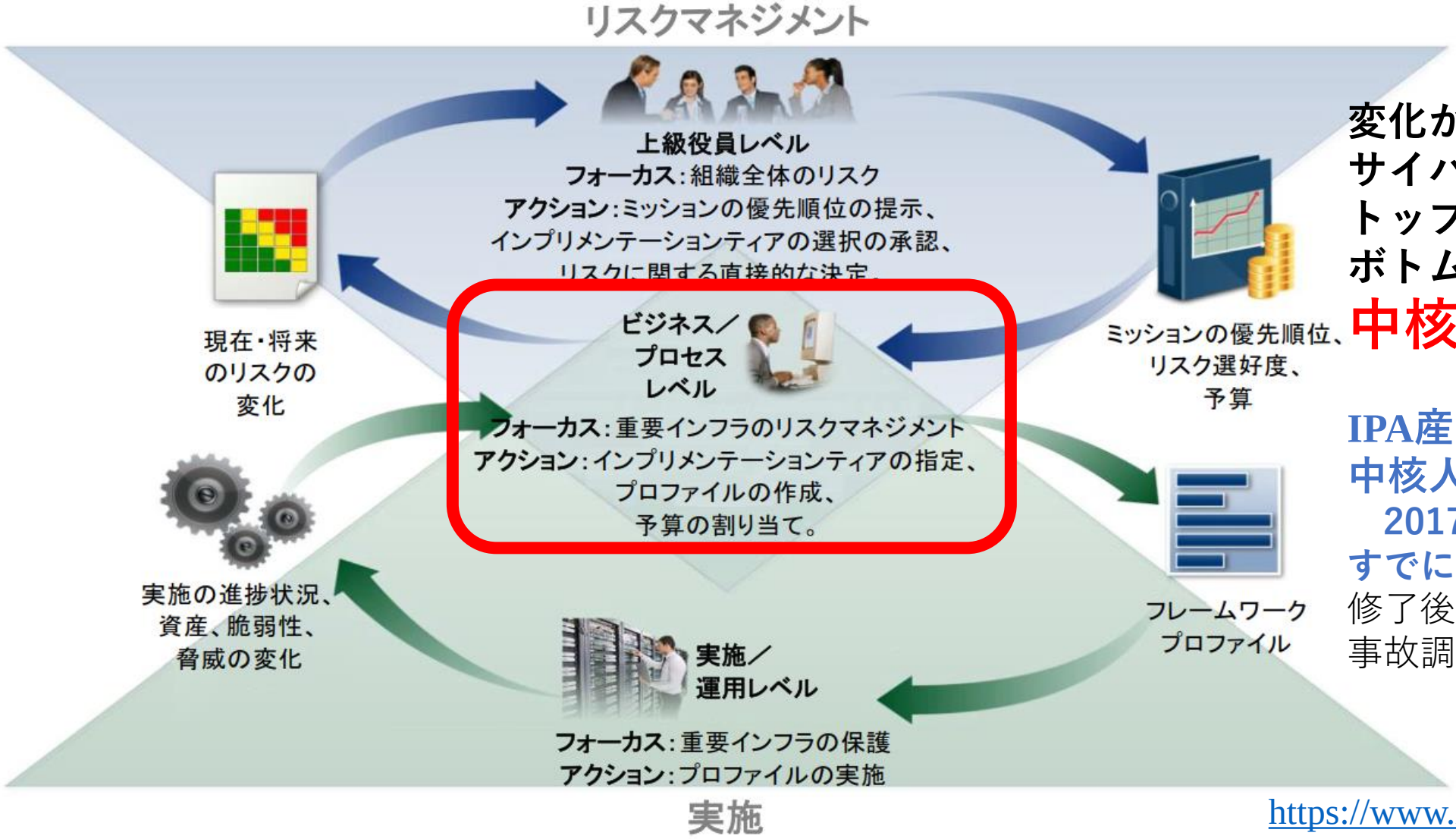
重要なスタッフとして仕事に組み入れるというスタンスが必要

OpenAI　Microsoft Copilot　Gemini

サイバーセキュリティプロジェクトの策定、進行の標準

2017年 オバマ大統領の指示で、NISTが組織的な取り組みの基本を策定（2023年ver.2発表）

Cybersecurity Framework (CSF)



変化が激しい
サイバーセキュリティは、
トップダウンだけでも
ボトムアップだけでも無理で、
中核組織が重要

IPA産業サイバーセキュリティ
中核人材育成プログラム
2017～進行中
すでに400名を超える修了生が
修了後、自社への貢献だけでなく、
事故調など国への貢献も期待

https://www.ipa.go.jp/files/000071204.pdf

日本のプロセス産業におけるサイバーセキュリティの課題

①自分のプラントがサイバー攻撃に襲われるわけがない？

日本でも、連日、被害の報道がなされている。それでも
「自分の会社を襲って、サイバー攻撃者になんの得があるの？」という声を聞く。

リスクを意識できなかったら、対策に魂が入るわけない！

②高圧保安法の改定で、サイバーセキュリティが必須に

サイバーセキュリティの審査は、KHKではなく、JQAが担当する。

プロセス安全の人間は、主体的にとりくむべきと考えているか？

③ビジネスの革新を実現するのに、サイバーセキュリティは必須

リモートワークやDXの推進で、アタックサーフェイスは広がり、
サプライチェーンとしての対策も必要になっている。
生成AIをビジネスに取りいれるにも、セキュリティの観点は必要である

サイバー攻撃の被害というリスクだけでなく、
ビジネスチャンスを失うリスクも認識すべき。

日本のプロセス産業におけるサイバーセキュリティの課題

①自分のプラントがサイバー攻撃に襲われるわけがない？

日本でも、連日、被害の報道がなされている。それでも
「自分の会社を襲って、サイバー攻撃者になんの得があるの？」という声を聞く。

リスクを意識できなかったら、対策に魂が入るわけない！

②高圧保安法の改定で、サイバーセキュリティが必須に

サイバーセキュリティの審査は、KHKではなく、JQAが担当する。

プロセス安全の人間は、主体的にとりくむべきと考えているか？

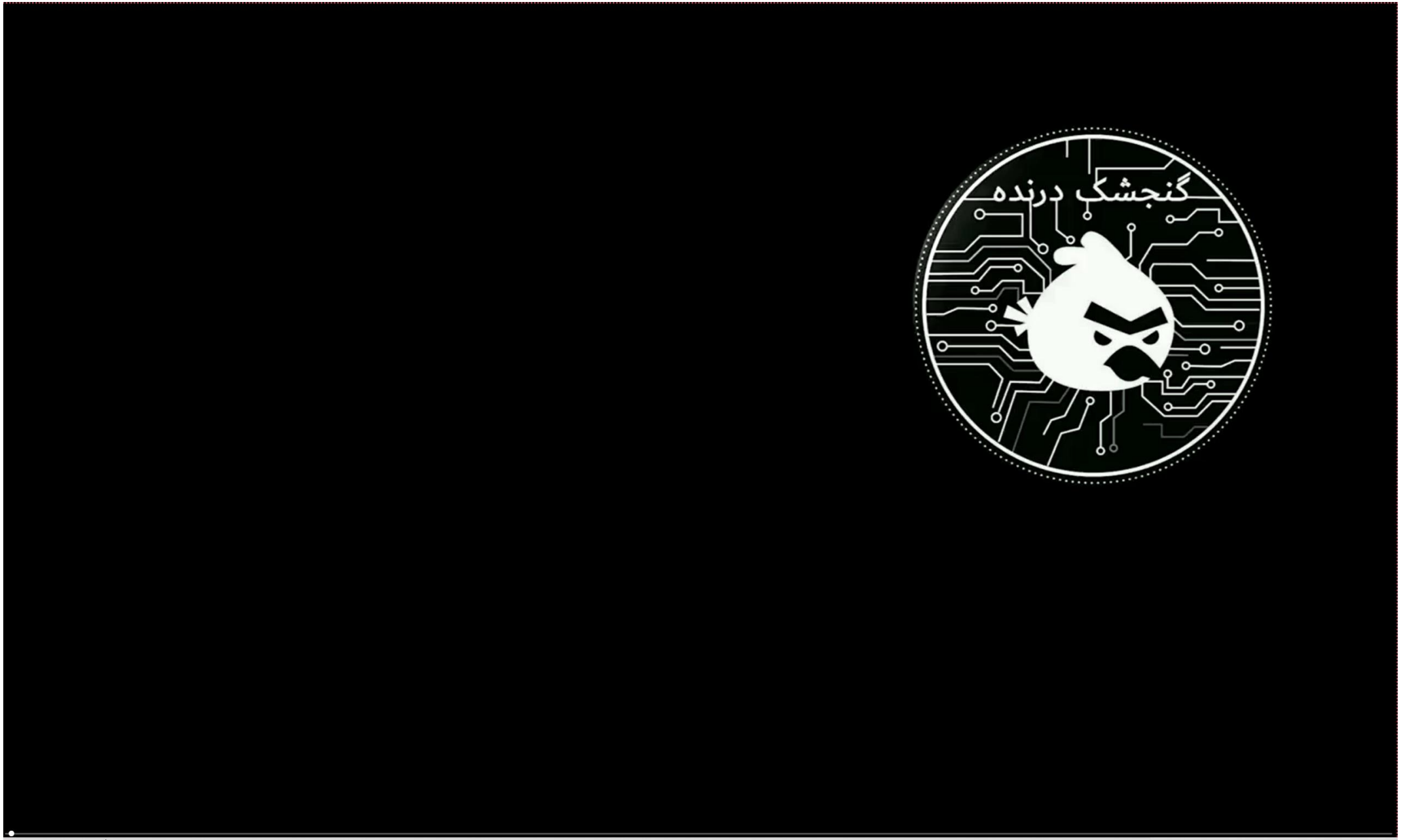
③ビジネスの革新を実現するのに、サイバーセキュリティは必須

リモートワークやDXの推進で、アタックサーフェイスは広がり、
サプライチェーンとしての対策も必要になっている。
生成AIをビジネスに取りいれるにも、セキュリティの観点は必要である

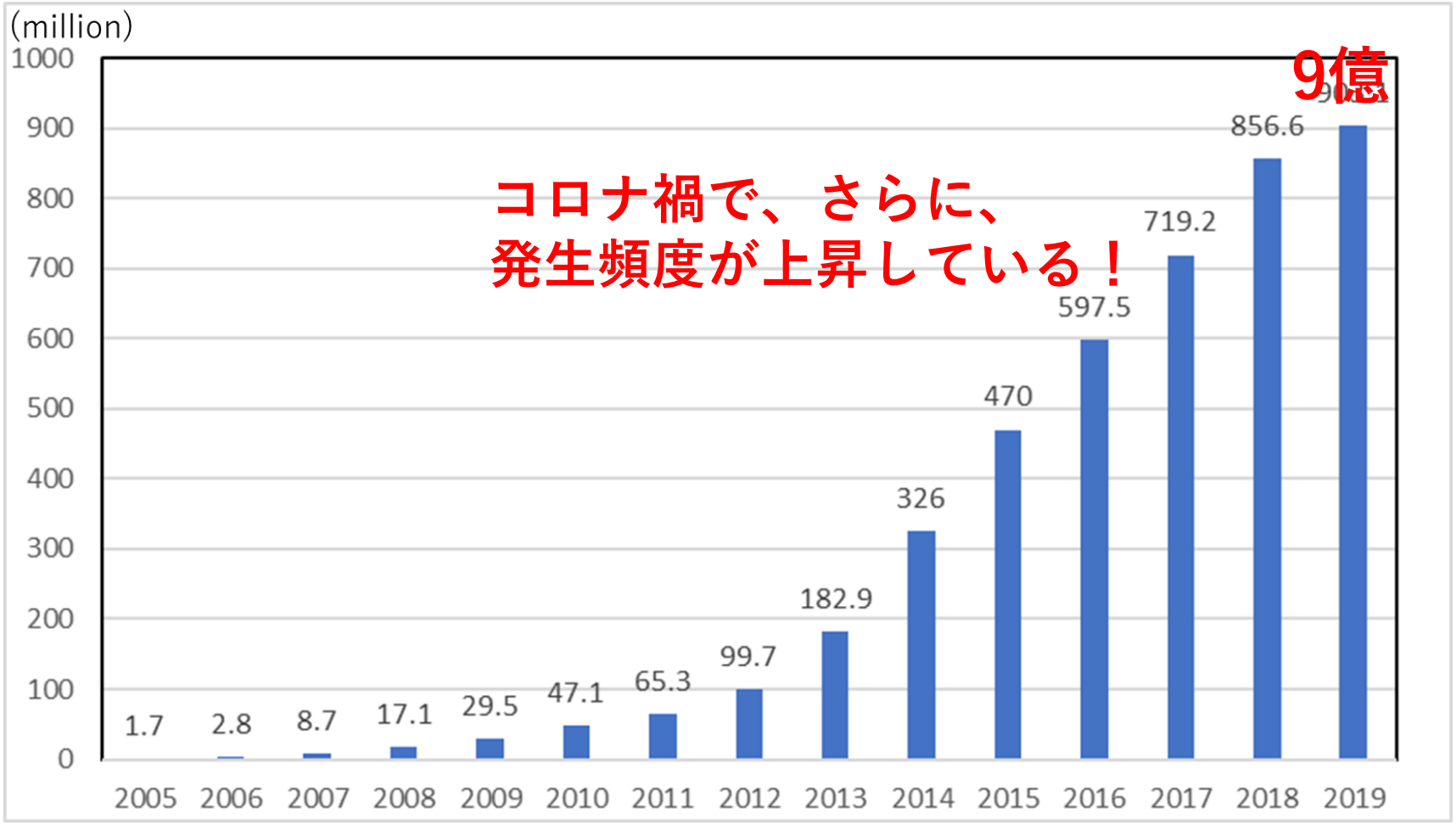
サイバー攻撃の被害というリスクだけでなく、
ビジネスチャンスを失うリスクも認識すべき。

まず、この動画をみていただきたい

https://x.com/GonjeshkeDarand/status/1541288345183158272?mx=2



アンチウィルスの検知率は実は驚くほど低い



コロナ禍で、さらに、
発生頻度が上昇している！

図１．1年間に新たに発生したマルウェアの種類数の推移
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/p

マルウェア発生
年間1億種類を
超える！
マルウェアは
検知されないことを
確認してから、
リリースされている

ランサムウェアは、
開発、配布、回収等が
分業化、システム化して
ブラックマーケットの
ビジネス形態が確立

私のところをサイバー攻撃して何の得が？

- **ランサムウェアは、ビジネスとしてシステム化されている。**
  - 世界中で、多くの支払いがされており、KADOKAWAも身代金を払ったという報道もある。
  - 少額要求のばらまき型から、標的を特定して多額の身代金を要求する形態に変化しているが、身代金が目的ではなく、破壊（あるいは情報搾取）が目的なランサムウェアも多い。
  - 機密情報を狙ったランサムウェアでは、機密情報が盗まれたか特定できないように破壊される。産業スパイの対象になるものが存在すれば、危険性はあると考えるべきでしょう。
- **サイバー攻撃者は大量に存在し、育成も実施している。**
  - 多くのプロ集団が存在し、育成の段階での力試しで、攻撃を実施する可能性がある。
  - これまでの愉快犯より、技術も、ねらう被害も高度化していると考えられる。
  - 攻めやすく、足がつきにくい相手であれば、だれでもよいかもしれない。
- **サイバー攻撃で株価を操作できる。**
  - 世の中には資金洗浄に株取引を利用する悪いファンドも存在する。
  - サイバー攻撃で大きな被害を起こせば、同業種の株価も連動して下がる可能性がある。
  - 先売りのタイミングは、事故が起こった直後でも、収益を確保できる。
  - サイバー攻撃者とファンドの協業は成立しうる。
  - サイバー攻撃の被害が株価に大きなインパクトを与えそうな相手であれば、だれでもよい。
  - 攻めやすく、足がつきにくい相手であれば、なおよい。
- **戦争やテロ行為の手段として、サイバー攻撃を利用。**
  - 遠隔から実施でき、被害も調整できるという利点がある。
  - サイバー攻撃の被害が社会に大きなインパクトを与えそうな相手であれば、だれでもよい。

防御が甘くて、監視もせずログも取っていない操業現場をもつインフラ事業者なら格好の標的

日本のプロセス産業におけるサイバーセキュリティの課題

①自分のプラントがサイバー攻撃に襲われるわけがない？

日本でも、連日、被害の報道がなされている。それでも
「自分の会社を襲って、サイバー攻撃者になんの得があるの？」という声を聞く。

リスクを意識できなかったら、対策に魂が入るわけない！

②高圧保安法の改定で、サイバーセキュリティが必須に

サイバーセキュリティの審査は、KHKではなく、JQAが担当する。

プロセス安全の人間は、主体的にとりくむべきと考えているか？

③ビジネスの革新を実現するのに、サイバーセキュリティは必須

リモートワークやDXの推進で、アタックサーフェイスは広がり、
サプライチェーンとしての対策も必要になっている。
生成AIをビジネスに取りいれるにも、セキュリティの観点は必要である

サイバー攻撃の被害というリスクだけでなく、
ビジネスチャンスを失うリスクも認識すべき。

1．②サイバーセキュリティに関する調査機関の指定について

第26回産業構造審議会 保安・消費生活用製品安全分科会
高圧ガス小委員会（ 2024年3月21日） 資料抜粋

- 経済産業大臣は、高圧ガス保安法第39条の16に基づき、高圧ガス保安協会又は経済産業大臣の指定する者に対し、認定基準に適合しているかどうかについて意見を聴取し、又は調査を依頼することができる。
- 本制度の認定要件を検査するため、サイバーセキュリティの専門性を有した組織を経済産業大臣の指定する者として指定する要件が必要であったことから、「高圧ガス保安法に基づく指定試験機関等に関する省令」（平成９年通商産業省令第23号。以下「指定則」という。）を改正し、**サイバーセキュリティに係る指定機関の要件を規定**した。
- 今般、**一般財団法人日本品質保証機構**より、**サイバーセキュリティに係る認定要件の調査を行う者**として指定申請等を受けたため、指定則に基づき審査を行ったところ、審査項目に適合していると評価できたことから、令和６年３月18日付けで**同機構の指定を行った**。

高圧ガス保安協会
又は別の組織（溶接協会？）
でも
サイバーセキュリティの審査はできない
という前提で
JQAが審査組織として
新たに選定された。

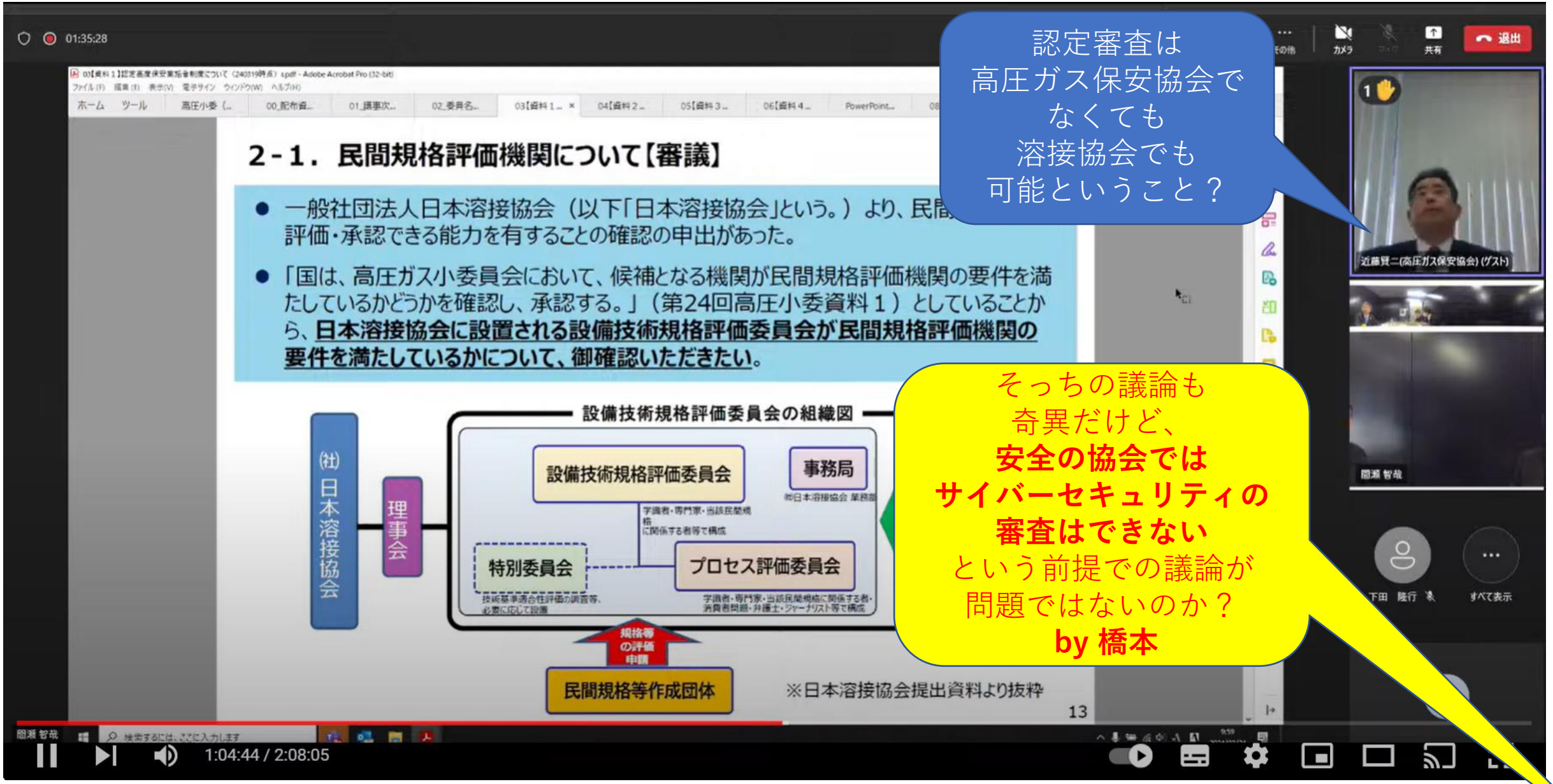
一般財団法人日本品質保証機構（JQA）

・設立：昭和32年（財団法人日本機械金属検査協会として設立し、平成23年に一般財団法人日本品質保証機構に移行）
・公正・中立な立場の第三者適合性評価機関
・情報セキュリティに関するISO/IEC 27001認証及びクラウドサービスセキュリティに関するISO/IEC 27017認証を実施
・ISO 9001、ISO 14001をはじめとするマネジメントシステム認証の総登録件数において、認証機関として国内最多の実績
・その他、国内外の法規制や認証制度の指定機関として、電気製品・医療機器・車載機器に関する電気安全の認証・試験、JISマーク認証等を実施

出典：一般財団法人日本品質保証機構（JQA） 総合案内、サービスハンドブック より抜粋・修正

資料1　認定高度保安実施者制度について（PDF形式：1,806KB）

https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/koatsu_gas/026.html



第26回産業構造審議会 保安・消費生活用製品安全分科会
高圧ガス小委員会（ 2024年3月21日）

ネットライブ中継

会議の様子は、以下の動画から御覧になれます。

動画

https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/koatsu_gas/026.html

日本のプロセス産業におけるサイバーセキュリティの課題

①自分のプラントがサイバー攻撃に襲われるわけがない？

日本でも、連日、被害の報道がなされている。それでも
「自分の会社を襲って、サイバー攻撃者になんの得があるの？」という声を聞く。

リスクを意識できなかったら、対策に魂が入るわけない！

②高圧保安法の改定で、サイバーセキュリティが必須に

サイバーセキュリティの審査は、KHKではなく、JQAが担当する。

プロセス安全の人間は、主体的にとりくむべきと考えているか？

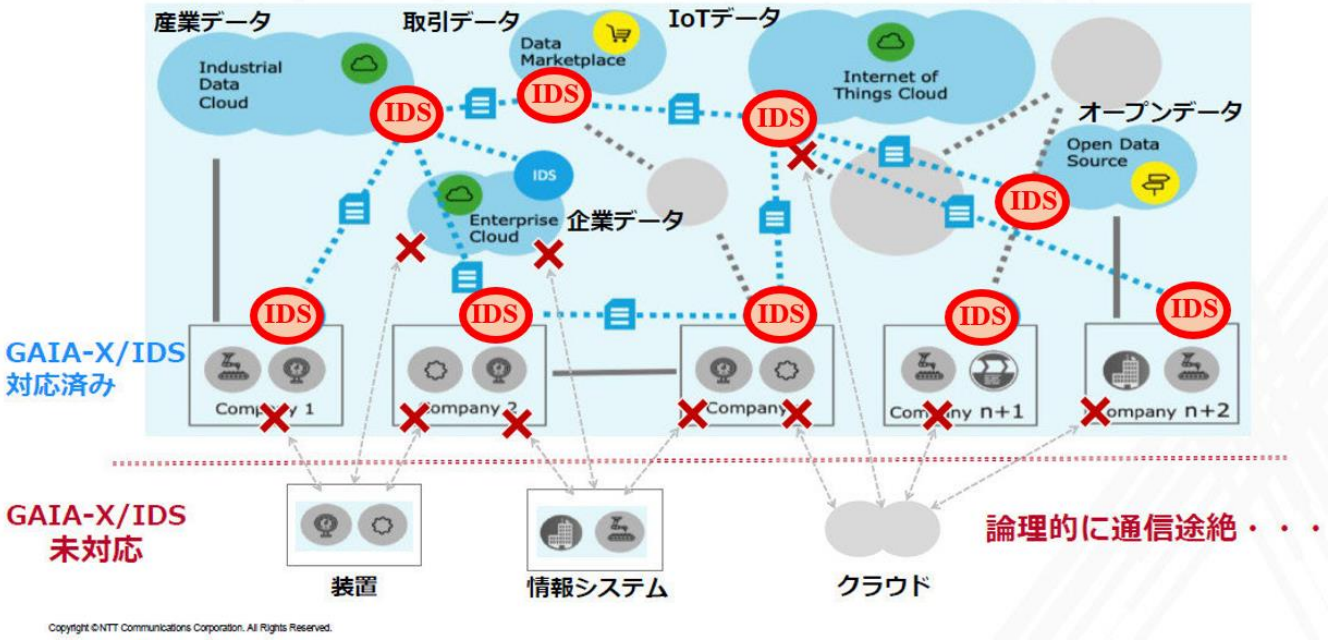
③ビジネスの革新を実現するのに、サイバーセキュリティは必須

リモートワークやDXの推進で、アタックサーフェイスは広がり、
サプライチェーンとしての対策も必要になっている。
生成AIをビジネスに取りいれるにも、セキュリティの観点は必要である

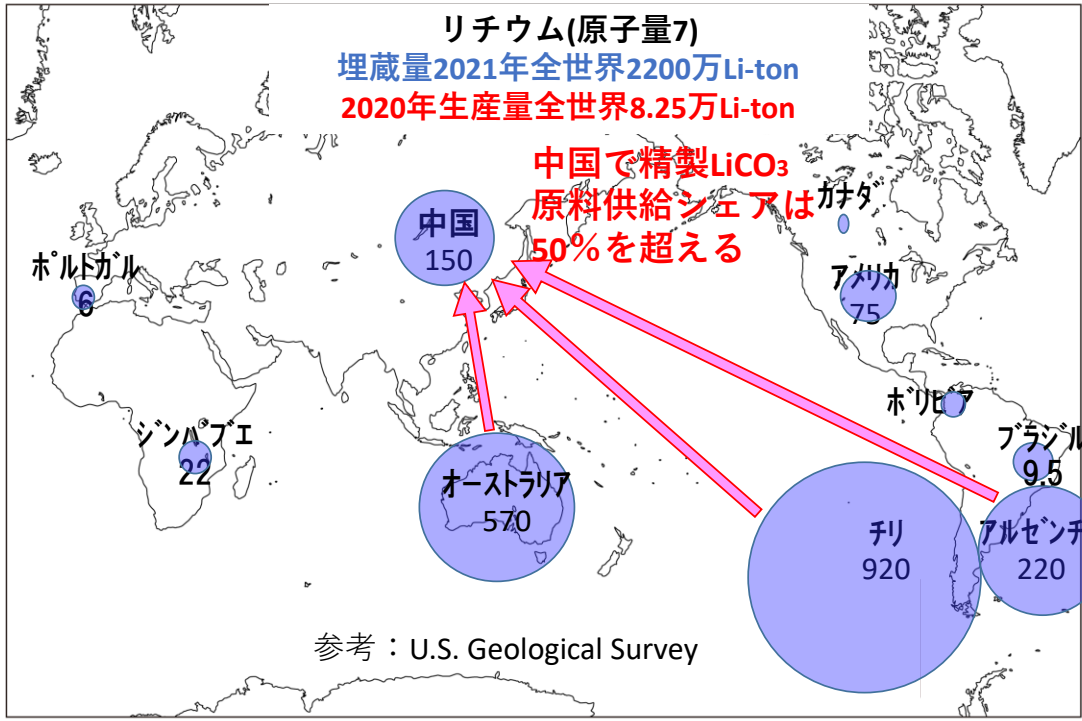
**サイバー攻撃の被害というリスクだけでなく、
ビジネスチャンスを失うリスクも認識すべき。**

EUバッテリー規制

- 電気自動車と産業用のバッテリは個別番号をもち、原料や製造時・輸送時のCO2排出量、リユースやリサイクルの情報が管理されなければならない（2026年施行）
- SIEMENSのGAIA-Xに対応したアプリでCO2のトレーサビリティを算出
- **GAIA-Xの世界でバッテリー市場を管理？**

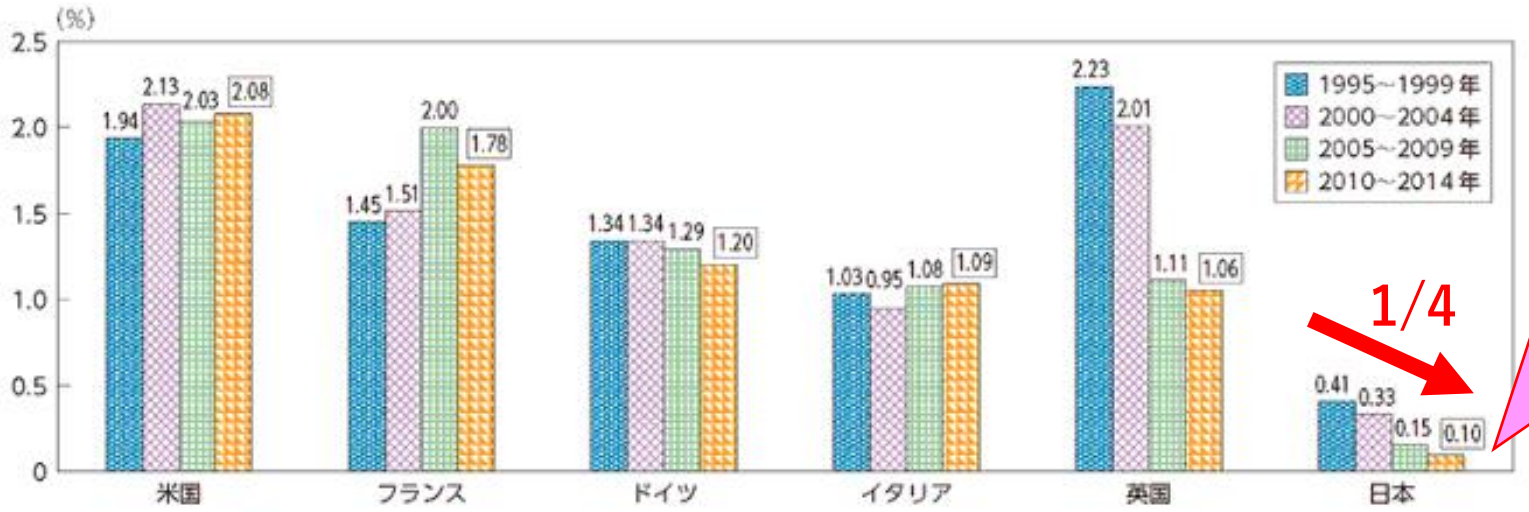


Copyright ©NTT Communications Corporation. All Rights Reserved.



近頃の若者は出世欲がない？

- 沈む船の席を奪いあってもしかたない。
- 周りの水位は上がっているのに、気づかない？
- 早く錨を切り離そうよ。次の大きな波で沈むかも。



資料出所　内閣府「国民経済計算」、JIP データベース、INTAN-Invest database を利用して学習院大学経済学部宮川努教授が推計したデータをもとに作成

（注）　能力開発費が実質 GDP に占める割合の５箇年平均の推移を示している。なお、ここでは能力開発費は企業内外の研修費用等を示す OFF-JT の額を指し、OJT に要する費用は含まない。

教育への公的支出も日本は
OECDでは38か国中37位
[OECD図表でみる教育2020]

アメリカの1/20！
コストカットばかりで
社員を大事にしない
経営者の姿勢が
暗黒の30年を
生んだのでは？

厚生労働省ホームページ　https://www.mhlw.go.jp/wp/hakusyo/roudou/18/backdata/2-1-13.html

伝えたいのは、
安全の人間が主体的にサイバー攻撃への防御を
検討してほしいという一点です。

プロセス安全は、サイバーセキュリティのイタチごっこに委ねない！

サイバー攻撃は、新たな手口が高頻度で現れ、
サイバーセキュリティはきりのない課題ですが、
プロセス安全への危険性もある問題です。
その防御を考えるのは、情報システム技術だけでは無理で、
従来の安全対策も有用です。

高圧ガス保安では、サイバーはわからないからＪＱＡという
安全側がサイバーの審査を投げ出した形になっていますが、
受審側は、OTとITが一体となって取り組んでくれることを祈っています。

by　橋本芳宏