第12回 Edgecross-GUTP/工場セキュリティガイドライン啓発・連続セミナ

# 重要インフラ事業者における工場セキュリティ課題と対策 ～サイバー事故調を例に～

2024/10/9

フォーティネットジャパン合同会社
OTビジネス開発部　小泉 和也

# フォーティネットは、世界最大規模のサイバーセキュリティ企業の1社です

設立：**2000年10月**

創設者：**Ken Xie、Michael Xie**

本社：**カリフォルニア州サニーベール**

NASDAQ上場（FTNT）：**2009年11月**

構成銘柄：**NASDAQ 100、S&P 500**

企業の持続可能性指標：
**2023年ダウ・ジョーンズ・サステナビリティ・インデックス（DJSI）のDJSI World（全世界対象）およびDJSI North America（北米地域対象）の構成銘柄に選定**

グローバルな顧客基盤

**775,000社以上**

顧客数

**50%以上**

全世界のファイアウォール出荷実績

2023年度の取扱高

**64億ドル以上**

（2023年12月31日現在）

**25億ドル以上**

2017年以降のイノベーションへの投資、91%を研究開発に投資

（2023年12月31日現在）

時価総額

**461億ドル**

（2024年6月30日現在）

証券投資適格格付け：

**BBB+**
**Baa1**

# 自己紹介

石油学会 設備維持管理士
(計装設備2016001号)

その他保有資格：
・一般計量士
・高圧ガス製造保安責任者　甲種機械
・危険物取扱者　甲種
・エネルギー管理士　熱分野
・公害防止管理者　大気１種／水質１種

## フォーティネットジャパン合同会社　OTビジネス開発部
## 小泉 和也 (Kazuya Koizumi)

これまで石油精製プラント(重要インフラ事業者)のエンジニアとして、OT現場の最前線で従事。
フィールド機器(Level0)から制御システム(Level1/2)までの幅広い領域に知識と経験を有する。
調節弁リモート診断の企画時、OTセキュリティの大切さと自身の知識ギャップを痛感した経験から、
より広くサイバー空間の「安全安心」と「便利さ」との両立に貢献するため、セキュリティ企業へ転身。

**Mission：「“安全安心”で“便利”なOTを、サイバーセキュリティで支える！」**

**＜経歴＞**

**2012年4月～2023年11月（11年）：**
**エネルギー企業にて、石油精製プラントにおける計測・制御設備(計装)担当エンジニア**
＋新設／改造／更新に関するエンジニアリング
＋トラブルシューティング、機器メンテナンス戦略の検討
＋新技術導入／DX案件の企画・検討・実行

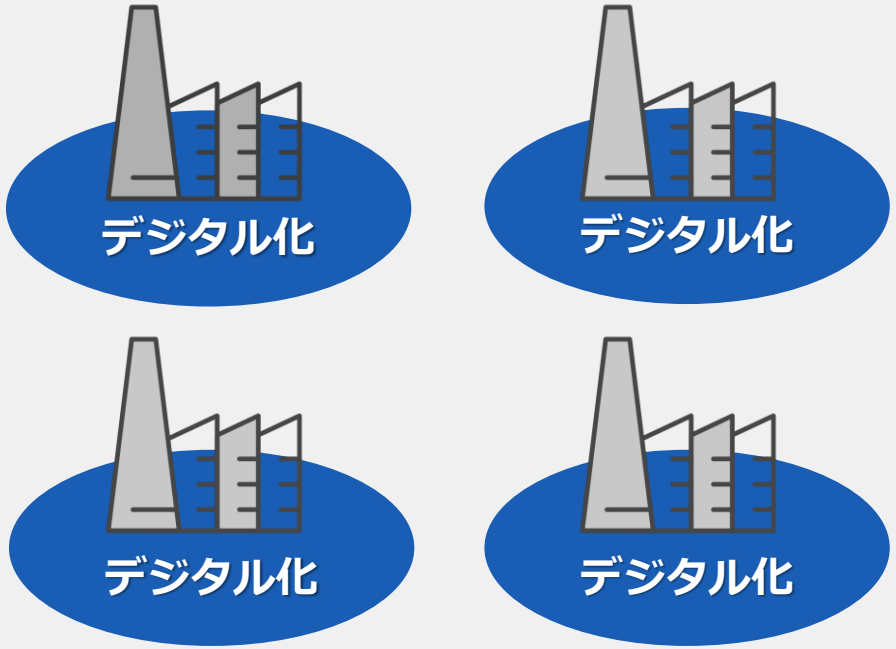
**2023年12月～現在：**
**フォーティネットジャパン合同会社にて、産業サイバーセキュリティのビジネス開発**

# Agenda

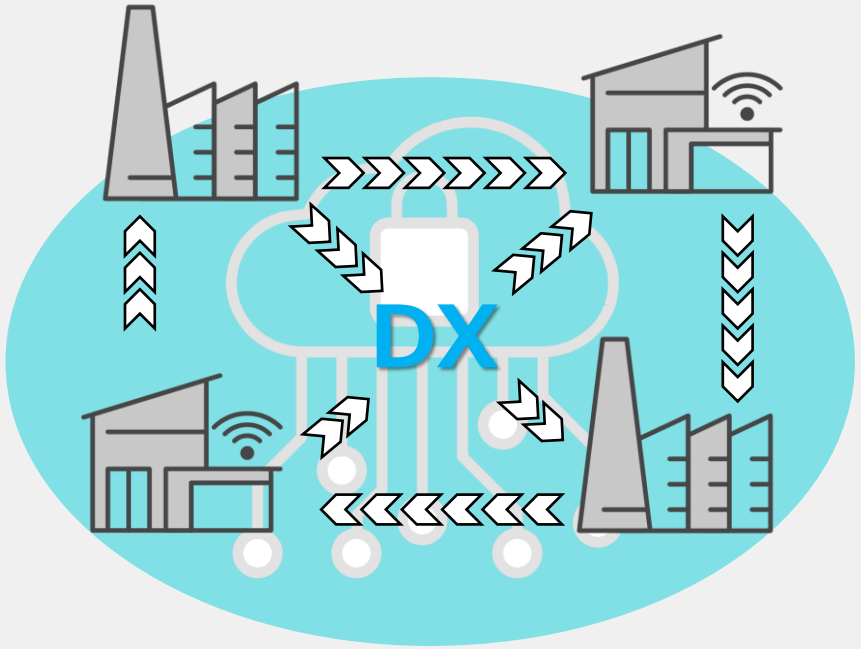
1. 重要インフラ事業者を取り巻く環境と課題感
2. “サイバー事故調”制度の概要
3. 「事故対応」のためのソリューション
4. まとめ

# 重要インフラ事業者を取り巻く環境と課題感

# つながる社会(DX社会)におけるOTセキュリティ対策




サイバーセキュリティ
リスクへの対処は
**自己責任**




サイバーセキュリティ
リスクへの対処は
**ビジネス参加条件**

**自社だけ守っていても守り切れない！**
**サプライチェーンに参加する企業としてOTセキュリティに対する実効性と説明責任が求められている**

# 経済安全保障推進法　第3章
# 基幹インフラ役務の安定的な提供の確保に関する制度の概要

## 基幹インフラ役務の安定的な提供の確保に関する制度の概要
（経済安全保障推進法 第３章）

### 趣旨

- 基幹インフラ役務（電気・ガス・水道等）の安定的な提供の確保は安全保障上重要。
- 基幹インフラの重要設備は役務の安定的な提供を妨害する行為の手段として使用されるおそれあり。
- 基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、重要設備の導入・維持管理等の委託を事前に審査。

### 概要

**１．基幹インフラ役務の安定的な提供の確保に関する基本指針を策定**

・対象事業者の指定に関する基本的な事項（当該指定に関し経済的社会的観点から留意すべき事項を含む）

・配慮すべき事項（重要設備等を定める主務省令の立案に当たって配慮すべき事項を含む）

・対象事業者その他の関係者との連携に関する事項　等

**２．審査対象**

**(1) 対象分野**（法律で対象事業の外縁を示した上で、政令で絞り込み）

| | | | | |
|---|---|---|---|---|
| 電気 | ガス | 石油 | 水道 | 鉄道 |
| 貨物自動車運送 | 外航貨物 | 航空 | 空港 | 電気通信 |
| 放送 | 郵便 | 金融 | クレジットカード | |

**(2) 対象事業者・・・主務大臣が指定**

・対象事業を行う者のうち、①重要設備（具体的な重要設備は主務省令で指定）の機能が停止・低下した場合に、②役務の安定的な提供に支障が生じ、③国家・国民の安全（国民の生存・社会経済秩序の平穏）を損なうおそれが大きいものとして主務省令で定める基準に該当する者

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai5/siryou8.pdf
https://www.meti.go.jp/policy/economy/economic_security/infra.pdf

### 特定社会基盤事業者の指定基準に該当すると見込まれる者　R５.10.4時点

| 対象分野（法律）／特定社会基盤事業の指定（政令） | | 特定社会基盤事業者の指定基準（省令） | 特定社会基盤事業者（※指定基準を踏まえ、対象となることが想定される者であり、現時点において指定を行った者ではありません。） |
|---|---|---|---|
| 電気 | 一般送配電事業 | 電気事業法第二条第一項第九号に規定する一般送配電事業者であること。 | 沖縄電力株式会社<br>関西電力送配電株式会社<br>九州電力送配電株式会社<br>四国電力送配電株式会社<br>中国電力ネットワーク株式会社<br>中部電力パワーグリッド株式会社<br>東京電力パワーグリッド株式会社<br>東北電力ネットワーク株式会社<br>北陸電力送配電株式会社<br>北海道電力ネットワーク株式会社 |
| 電気 | 送電事業 | 電気事業法第二条第一項第十一号に規定する送電事業者であること。 | 電源開発送変電ネットワーク株式会社<br>福島送電株式会社<br>北海道北部風力送電株式会社 |
| 電気 | 配電事業 | 電気事業法第二条第一項第十一号の三に規定する配電事業者であること。 | 指定事業者なし<br>（現在営んでいる事業者が存在しないため） |

| 対象分野（法律）／特定社会基盤事業の指定（政令） | | 特定社会基盤事業者の指定基準（省令） | 特定社会基盤事業者（※指定基準を踏まえ、対象となることが想定される者であり、現時点において指定を行った者ではありません。） |
|---|---|---|---|
| 電気 | 発電事業 | 電気事業法第二条第一項第十五号に規定する発電事業者であって、出力五十万キロワット以上の発電等用電気工作物を有すること。 | 鹿島パワー株式会社<br>株式会社コベルコパワー神戸<br>株式会社コベルコパワー神戸第二<br>株式会社コベルコパワー真岡<br>株式会社JERA<br>関西電力株式会社<br>九州電力株式会社<br>四国電力株式会社<br>常磐共同火力株式会社<br>相馬共同火力発電株式会社<br>中国電力株式会社<br>中部電力株式会社<br>電源開発株式会社<br>東京電力ホールディングス株式会社<br>東京電力リニューアブルパワー株式会社<br>東北電力株式会社<br>勿来IGCCパワー合同会社<br>日本原子力発電株式会社<br>日本製鉄株式会社<br>姫路天然ガス発電株式会社<br>広野IGCCパワー合同会社<br>福島ガス発電株式会社<br>北陸電力株式会社<br>北海道電力株式会社<br>三菱重工業株式会社 |

# 直近のサイバーセキュリティ関連の政策動向

## 企業のセキュリティ対応力格付け制度

### サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討

実効性強化

- これまで「サイバーセキュリティ経営ガイドライン」や産業分野別のガイドライン等を整備し、各企業等による積極的な取組を推進してきたところ。他方、**異なる取引先から様々な対策水準を要求される**といった課題や、**外部から各企業等の対策状況を判断することが難しい**といった課題は依然として存在。
- 今後は、諸外国で議論が進んでいる、「サイバー対策」のレーティング等も参考にしつつ、**各企業等の業種・規模などのサプライチェーンの実態を踏まえた満たすべき各企業の対策のメルクマール**や、**業界間の互換性を確保しながら**その**対策状況を可視化する仕組みを検討していく。**
- 併せて、関係省庁とも連携し**政府機関・企業による活用を促す枠組みと紐付ける**ことで、**その実効性を強化**していく。

**想定される検討事項**

- **既存のガイドライン等をIPAが一元的に管理・体系化し、企業のセキュリティ対策基準を明確化できないか**
- 既存ガイドライン等と整合を取りつつ、**業種横断的なセキュリティ対策レベルを評価（自己評価、第三者認証）できないか**
- 政府機関等における**調達要件**や、サプライチェーン上の取引先や投資家等の**ステークホルダとの対話※での活用**を促進し、**実効性の強化**につなげられないか

※サイバーセキュリティへの取組に関し、投資家を含むステークホルダと企業経営者との対話（開示）の在り方等についても検討が必要ではないか。

**対策レベルの可視化（イメージ）**

| 成熟度の定義 | 三つ星（★３） | 四つ星（★４） | 五つ星（★５） |
|---|---|---|---|
| レベル感の説明 | サプライチェーン形成企業として最低限満たすべき基準 | サプライチェーン形成企業として標準的に満たすべき基準 | 重要インフラ事業者、経済安全保障上、特に重要なインフラ事業者、関連サプライヤーが満たすべき基準 |
| ガイドラインの相当性を認定 | ・IPA「中小企業の情報セキュリティ対策ガイドライン」 | ・○○業界ガイドライン<br>・・・・ | ・重要インフラ行動計画<br>・・・・ |
| ガイドライン準拠を確認する方法を定義 | 自己宣言型 | 第三者認証型 | 第三者認証型 |

政府調達・補助施策等への要件化

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

17

## 重要インフラ・インシデント報告義務

4　政府の情報提供・対処を支える制度

① インシデント報告の義務化について

- 国民生活及び経済活動の基盤である重要インフラ事業者に対するインシデント報告義務化は導入すべき。
- 報告を義務化する範囲については、ある程度広くあるべき。
- 重要インフラのデジタル技術への依存度が増していることを踏まえれば、デジタル・インフラストラクチャーと電力は特に重要なインフラとして扱うべき。
- 非重要インフラについて、海外の事例等も参考に、ソフトウェアベンダー、防衛産業、重要製造業など、特に重要な者に対しては、報告の義務化などを適用してもいいのではないか。

② インシデント報告の迅速化について

- 行政へのインシデント報告は、これまで監督省庁へ行われてきたが、セキュリティ担当者のリソースの不足からリアルタイム性が損なわれる可能性がある。これをなくすために報告先の一元化を含めて工夫してほしい。
- 事業者に負担をかけずに効率的に情報収集し、フィードバックするという仕組みが重要になってきている。サイバー攻撃の情報共有は数分、数十分程度でやる必要があるため、迅速であることが重要。そのための鍵は自動化であり、自動化は効率化にも寄与する。

「サイバー安全保障分野での対応能力の向上に向けた有識者会議官民連携に関するテーマ別会合」資料より抜粋

**平時・インシデント発生時の双方で「説明責任」がさらに求められる方向性**




https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/008_03_00.pdf　https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai3/siryou4-2.pdf

# エネルギー業界に見るOTセキュリティ関連法改正 (2023年12月21日施行)

経済産業省
Ministry of Economy, Trade and Industry

## <サイバー事故調>

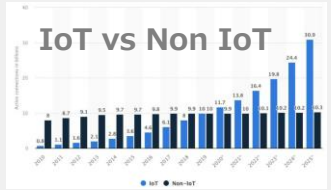
**「高圧ガス保安法等の一部を改正する法律案」が閣議決定されました**
(ニュースリリース 2022年3月4日)

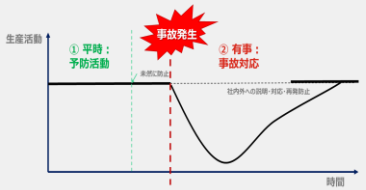
参照：*https://www.meti.go.jp/press/2021/03/20220304004/20220304004.html*

“あわせて、**サイバーセキュリティに関する重大な事案**が生じた場合に、国が独立行政法人情報処理推進機構に**原因究明の調査を要請することができる**こととします。”（「情報処理の促進に関する法律」の改正）

**<法改正の背景として>**

- **スマート保安の促進**
  **工場・プラントのデジタル化、クラウド活用**
- **新たな保安上のリスク分野への対応**
  **ITセキュリティとOTセキュリティのリスクの考え方の違い**
- **災害対策・レジリエンスの強化**
  **① 予防と事故対応の考え方**
  **② BCP対応との連携**




## <認定基準改定>

**認定高度保安実施事業者制度の運用を開始し、燃料電池自動車等の規制の一元化を実施しました**
(ニュースリリース 2023年12月21日)

参照：*https://www.meti.go.jp/press/2023/12/20231221003/20231221003.html*

**認定の基準に「サイバーセキュリティの確保」が新設**され、下記いずれかのガイドラインを参考にPDCA構築が求められるようになりました。

**<改正等を行う対象法令と関連ガイドラインの位置づけ>**

- **高圧ガス保安法**
  - **工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン** 他
- **ガス事業法**
  - 業界関連各ガイドライン
- **電気事業法**
  - スマートメーターガイドライン
  - **電力制御システムセキュリティガイドライン**
  - **自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（電気事業以外）**

# 重要インフラ事業者が感じる課題感①：説明責任と実効性の両立

“説明責任“も重視される時代ですが・・・”実効性”を忘れずに！

## 説明責任

- 規制/ガイドラインへの適合
- ルールの制定、文書化

▼

**形骸化に注意**

“経済産業省のガイドラインに
適合しています！”

## 実効性

- ルールの順守状況
- 運用コスト含む効率性
- リスク評価に応じた濃淡

▼

**「組織」「運用」「技術」のバランス**

“経済産業省のガイドラインを参考に
自社のリスク応じた対策に
落とし込んでいます！”

**現場の事業被害リスクの低減が目的。ガイドライン適合はその手段。**

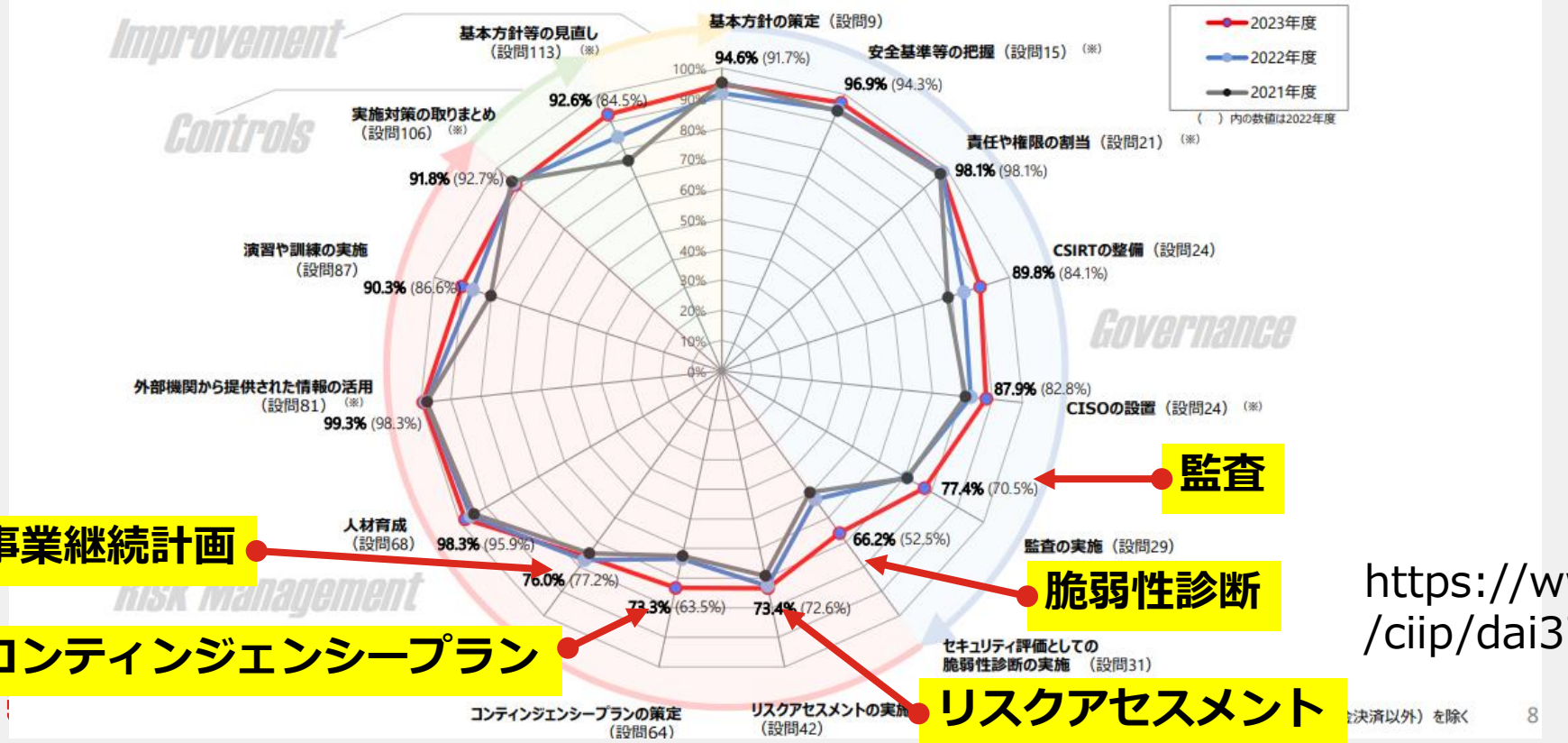
# 重要インフラ事業者が感じる課題感②：「事故対応」対策

## NISC：重要インフラにおける安全基準等の浸透状況に関する調査について［2023年度］

### （参考）調査結果の経年比較

NISC

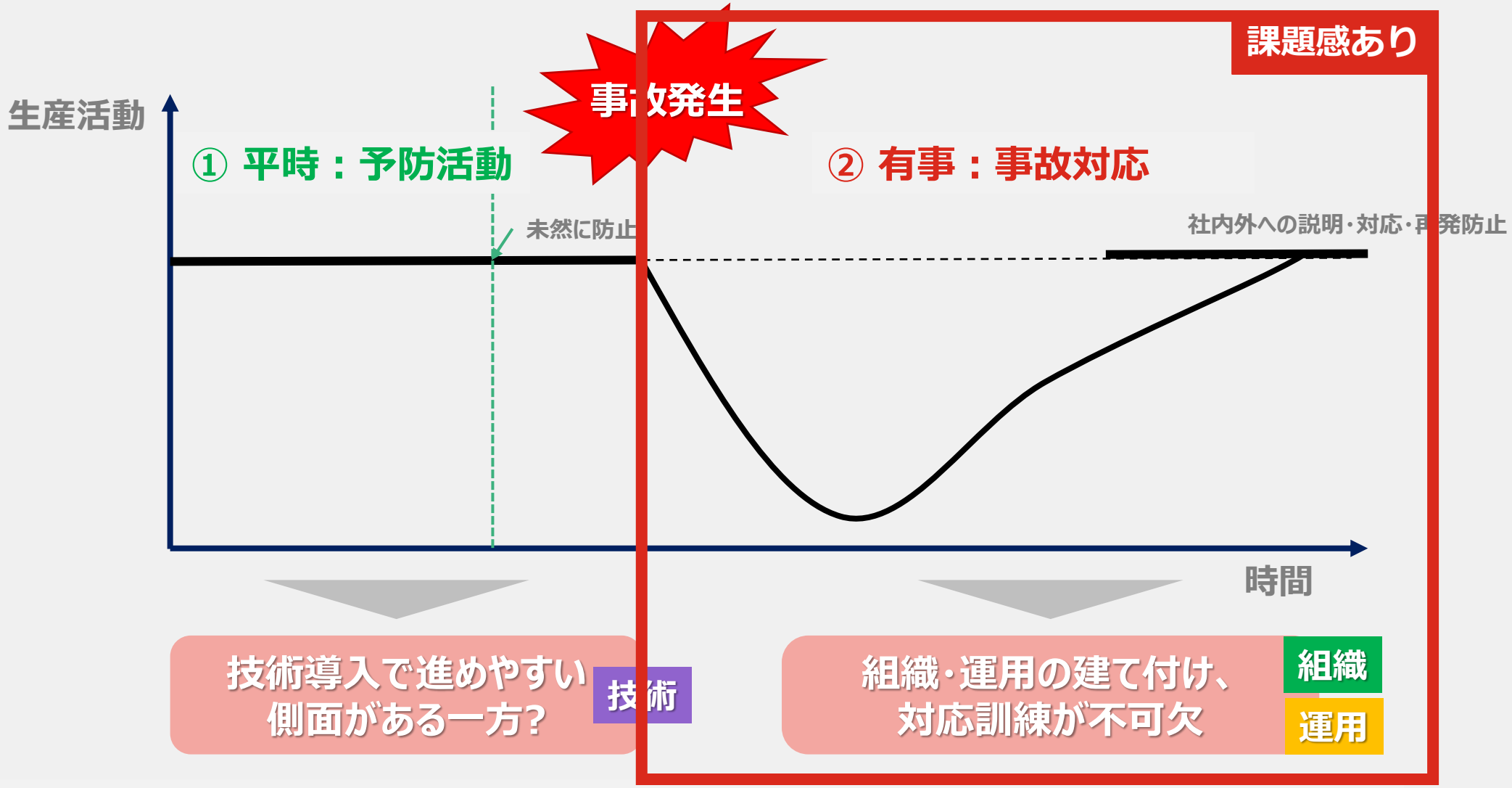
- **セキュリティ対策の実施状況は多くの項目において高い水準で推移**しており、安全基準等は浸透しつつあると評価できる。
- 「CSIRTの整備」「CISOの設置」「監査の実施」「脆弱性診断の実施」といった**組織統治に関する項目の実施率について改善**が見られ、 経営層の責務において実施すべき取組に進展が見られる。
- 「コンティンジェンシープランの策定」「基本方針等の見直し」といった**リスクマネジメント及び改善における取組の実施率に向上**が見られ、レジリエンス向上への取組の進展が見られる。
- しかし、 リスクマネジメントに係る項目である**「脆弱性診断の実施」「リスクアセスメントの実施」「事業継続計画の策定」等の実施率は、７割前後**であり、これらを改善していくことが今後の課題である。




https://www.nisc.go.jp/pdf/council/cs/ciip/dai37/37_shiryou3_shintou.pdf

# 重要インフラ事業者が感じる課題感②：「事故対応」対策

OTセキュリティのやることは２つ、①平時の予防活動と②有事の事故対応

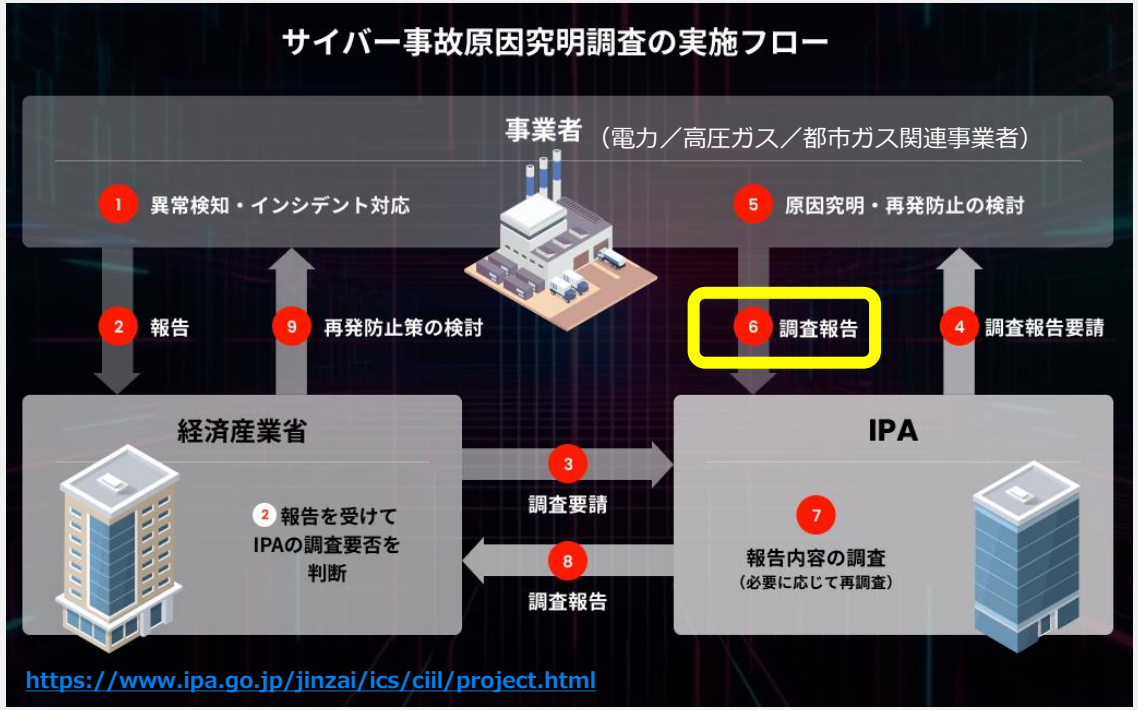



**サイバー空間を安心・安全に保つことで「事業被害リスクの低減」に貢献**

# “サイバー事故調”制度の概要

# “サイバー事故調“制度について

## IPA調査分析部サイバーインシデント調査室ウェブサイトより




**書面調査** → 十分に原因の究明が図られなかった場合 → **現地調査**

**<報告書項目 *2>**

1. **システム構成**
2. **情報セキュリティ管理体制**
3. **サイバー事故の概要、被害及び経緯**
4. **サイバー事故の技術的・組織的要因**
5. **再発防止策 (事業者考案)**
6. **再発防止策への評価（必要に応じ、より適切な再発防止策を経産省が提言）**

**（IPAによる立入調査）**

**<サイバー事故原因究明実施フロー>**

① 異常検知、事業者によるインシデント対応

② 事業者から経産省へ報告 (サイバー要因の可能性がある旨を記載)

② 経産省がIPAの調査要否を判断 (調査不要の場合はここで完了)

**or**

③ 経済産業省からIPAに調査要請

④ IPAから事業者に調査報告要請 *2

⑤ 事業者にて原因究明・再発防止の検討

⑥ **事業者からIPAに調査報告(書面調査)**

・・・ 事故詳細を記載した「インシデント調査報告書」

⑦ IPAにて報告内容の調査、**必要に応じて再調査実施(現地調査)**

・・・ ⑥ 書面調査により十分な原因究明が図られなかった場合、現地調査（ログの収集及び解析等）を実施

⑧ 最終調査終了後、IPAから経産省へ調査報告書を提出

⑨ 経産省は調査報告を踏まえ、再発防止策の検討(報告書項目6項参照)を行う

# サイバー事故調の調査対象として想定される事案

## 現時点では、エネルギー関係の事業者が対象・・・将来は？

| 調査対象事業者 | | 調査対象として想定される事案 |
|---|---|---|
| 電気<br>**電力(発電・送配電)** | 一般送配電事業者<br>大規模発電事業者<br>認定高度保安実施設置者 | 電気関係報告規則第３条において報告義務が課されている事故のうち、<br>サイバー攻撃に起因するおそれがあるもの |
| 高圧<br>**石油・化学** | 第一種製造事業者 | 高圧ガス・石油コンビナート事故対応要領において報告義務が課されている事故のうち、<br>サイバー攻撃に起因するおそれがあるもの |
| ガス<br>**都市ガス** | 認定高度保安実施ガス小売事業者<br>認定高度保安実施一般ガス導管事業者<br>認定高度保安実施特定ガス導管事業者<br>認定高度保安実施ガス製造事業者<br>一般ガス導管事業者<br>ガス製造事業者 | ガス関係報告規則第４条において報告義務が課されている事故のうち、<br>サイバー攻撃に起因するおそれがあるもの |

IPA 調査分析部サイバーインシデント調査室ホームページより
https://www.ipa.go.jp/jinzai/ics/ciil/project.html

# 米国LNG基地における爆発事故(2022年)

## “サイバー事故調”の対象になりそうな事故の例として・・・

✅ 2022年6月8日、米国の20%のLNG処理を担う Freeport LNG のテキサス州の設備で爆発事故発生。2023年2月まで生産停止。

✅ CO, $N_2O$, $SO_2$ などの有害物質を放出したと推定。

✅ ロシアのサイバー偵察活動が観測されていたことから、**当初はサイバー攻撃ではないかとの説もあった**。OTネットワーク内の監視ソリューションがなかったため、XENOTIMEの**サイバー攻撃手法の検知ができない**とされた。



https://www.reuters.com/business/energy/explosion-hits-freeport-lng-plant-us-natgas-prices-plunge-2022-06-08/

https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2023-02/PHMSA-FERC-USCG%20Feb%2011%202023%20Freeport%20Information%20Session%20Presentation%20%28002%29_0.pdf

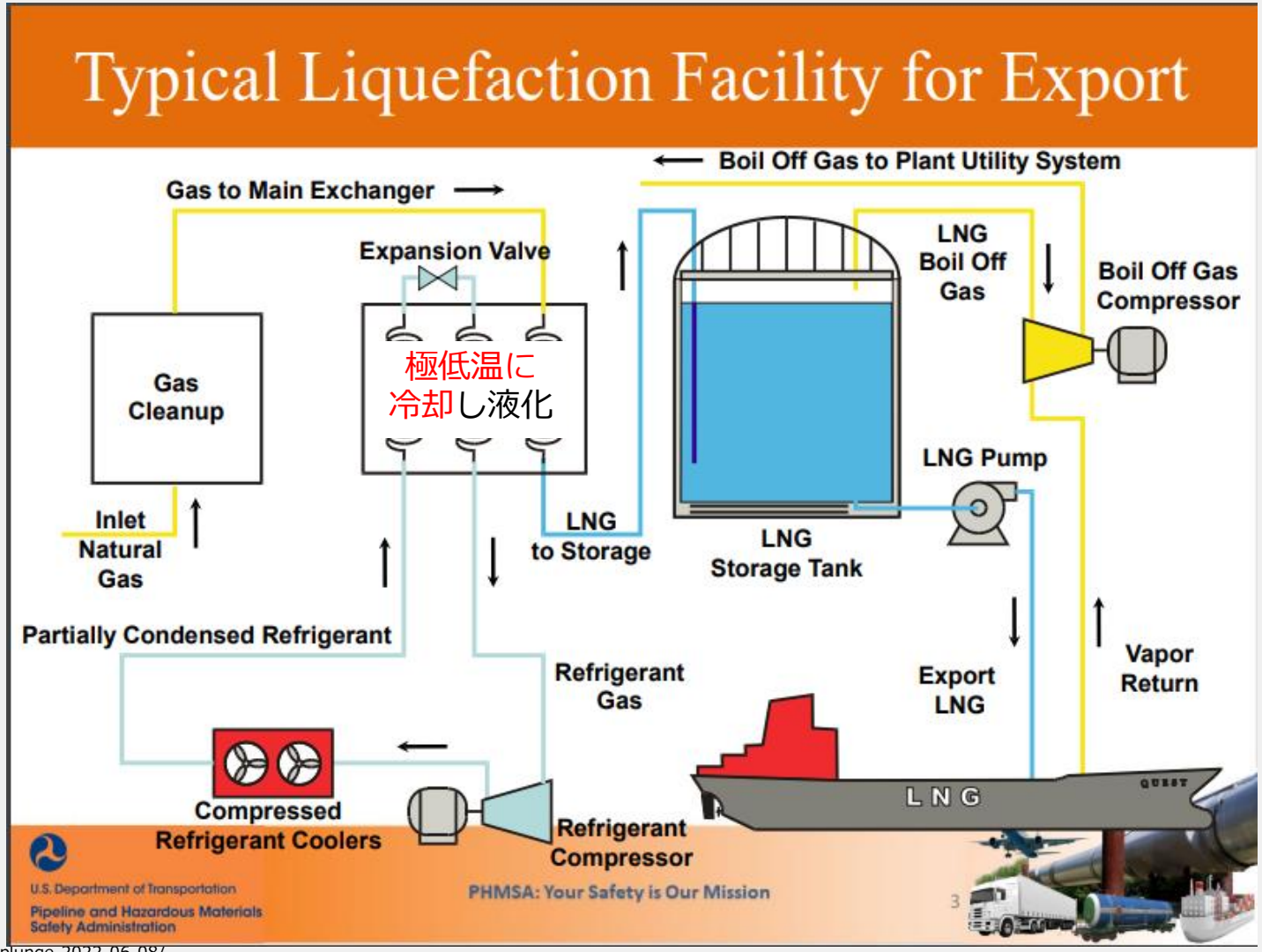
# 米国LNG基地における爆発事故(2022年)

“サイバー事故調”の対象になりそうな事故の例として・・・

✅ 2022年6月8日、米国の20%のLNG処理を担う Freeport LNG のテキサス州の設備で爆発事故発生。2023年2月まで生産停止。

✅ CO, $N_2O$, $SO_2$ などの有害物質を放出したと推定。

✅ ロシアのサイバー偵察活動が観測されていたことから、**当初はサイバー攻撃ではないかとの説もあった**。OTネットワーク内の監視ソリューションがなかったため、XENOTIMEの**サイバー攻撃手法の検知ができない**とされた。




https://www.reuters.com/business/energy/explosion-hits-freeport-lng-plant-us-natgas-prices-plunge-2022-06-08/

https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/2023-02/PHMSA-FERC-USCG%20Feb%2011%202023%20Freeport%20Information%20Session%20Presentation%20%28002%29_0.pdf

# 米国LNG基地における爆発事故(2022年)

**直接原因**：液封状態(缶詰状態)になったLNGの過圧によるBLEVE(沸騰液膨張蒸気爆発)

極低温LNG配管系が、缶詰状態 → 外気温の影響で系内の温度上昇 → 沸点を超えて気化、LNG沸騰 → 配管過圧、破損により外部漏洩 → 配管内LNGが一気に気化(BLEVE) → 周辺の着火源で引火し、大爆発

逃げ道なし！

https://ja.wikipedia.org/wiki/%E3%83%95%E3%82%A1%E3%82%A4%E3%83%AB:Bleve_explosion.png

**根本原因**：

1. 圧力安全弁の検査手順、および、開閉操作禁止弁 (Car Seal Valve)の管理手順不備
2. 極低温配管の温度上昇アラームの設定不備
3. LNGを液封状態にしうる弁が、オペレーターの裁量で操作できた運転手順不備

http://www.newsrouter.com/Newsrouter_uploads/77_New/news_release.asp?intRelease_ID=9752&intAcc_ID=77

**管理手順の不良により、ヒューマンエラーの歯止めがなく、そのまま事故に至った**

**（結局は違ったが）サイバー要因が疑われていたこの事案・・・事故調査はどうだった？**

# 「事故対応」のためのソリューション

# サイバー事故調ソリューション構成

## ① 事故調査に必要なログをワンストップで提供可能なソリューションを構想

セキュリティログを収集することでサイバー事故か否かの切分け、サイバー要因の際の分析情報として活用

| 設備稼働情報 | サイバーセキュリティ・関連情報 | 物理セキュリティ・関連情報 |
|---|---|---|
| プラント稼働・異常状況 | サイバーセキュリティ原因 | 物理セキュリティ |
| | ✓ USBメモリ接続 | ✓ 入退館IDチェック |
| | ✓ 管理外のPC接続 | ✓ 不正侵入検知 |
| | ✓ 脅威検知 | |
| | ✓ 設定・構成変更履歴 | |

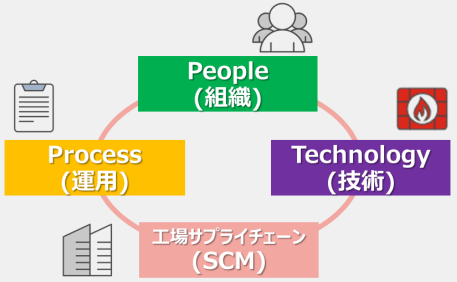
サイバー要因か否か切分け

OTセキュリティモニタリングと事故調査への備え

## ② OTセキュリティ管理体制の構築支援（アセスメント／コンサルティング）

事故発生を起点とした責任組織や運用ルール、訓練、そしてSCM管理を含めたOTセキュリティ体制支援

| 書面調査内容 *2 | 対応ソリューション |
|---|---|
| ①システム構成 | アセスメント／コンサルティング（OTセキュリティ管理体制の構築支援） |
| ②情報セキュリティ管理体制 | |
| ③事故の概要、被害及び経緯 | 脅威の入口から想定されるリスク要因分析 |
| ④事故の技術的・組織的要因 | |
| ⑤再発防止策 | ー （④内容の裏返し） |




IPA立入調査への備えと事故対応体制構築

# 技術だけじゃないフォーティネットのOTセキュリティ戦略

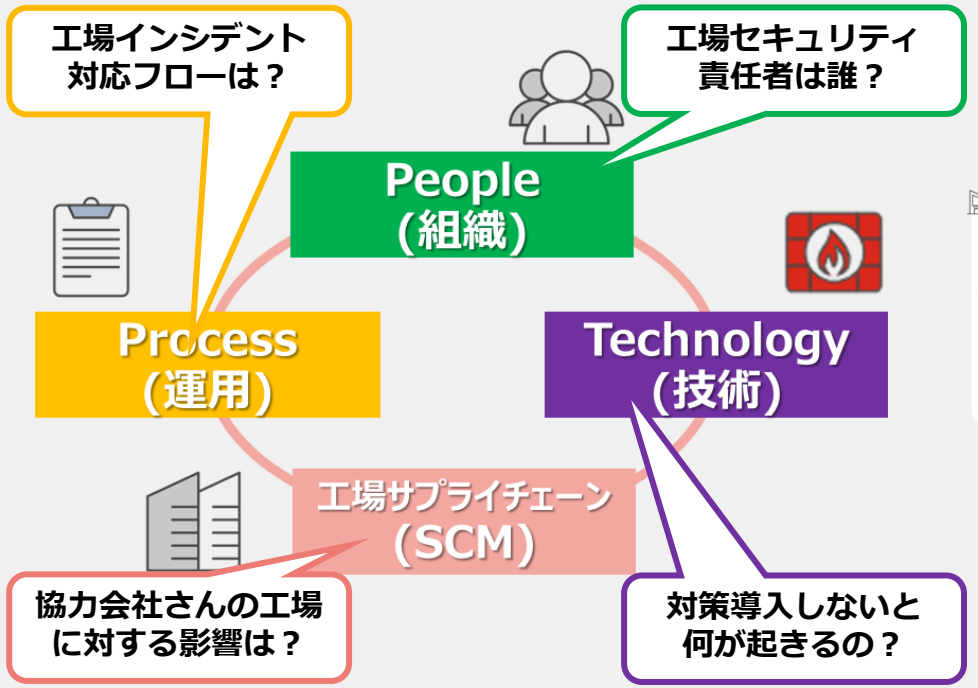
## 現状把握からサプライチェーン強化までワンストップで支援

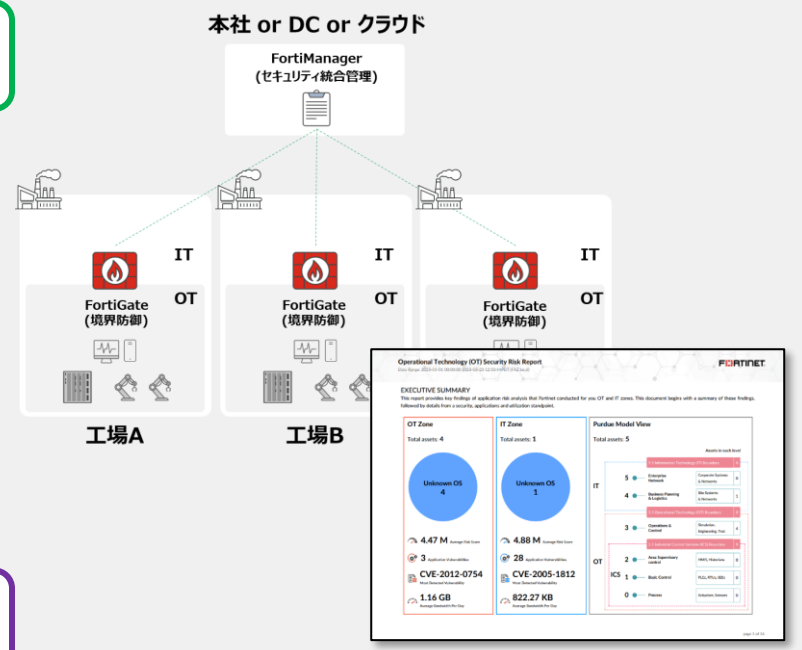
① 現状把握

② リスクの正しい理解と計画

③ ソリューション導入
(モデル工場へ)

④ 全拠点展開&サプライチェーン


**OTセキュリティ簡易診断**

まずはWeb問診、
「説明責任」、「実効性」の両輪を実現

**アセスメントとコンサルティング**

ITとOTのリスクの違いを認識し、
自分事となれる仕組みづくり

**OTセキュリティレベルの底上げ**

得られたノウハウを活用、
自社ベストプラクティスで横展開

# OTセキュリティ対策と進め方

## 経産省ガイドラインを活用して組織・運用・技術・SCMをバランスよく対策することで実効性のあるOTセキュリティを実現





**経済産業省工場セキュリティガイドラインで対策実施**
**先ずは 評価 ALL「B」を目指す**

| PPT項目 | サブ項目 | 評価「B」達成に必要な成果物 | 各項に対するFTNTソリューション | | |
|---|---|---|---|---|---|
| 組織（People） | ガバナンス体制 | 組織体制「役割」、「機能」の定義<br>組織体制キャリアパスの定義 | コンサルティング | | 予防 / 事故対応 |
| | 現場教育 | 現場向けサイバーセキュリティ教育プログラム | コンサルティング | | 予防 / 事故対応 |
| 運用（Process） | 定期評価 | 定期評価手順書 | コンサルティング、脆弱性情報の把握 | OT-IDS | 予防 |
| | インシデント対応 | インシデント対応手順書 | コンサルティング | | 事故対応 |
| | 資産管理 | 工場システムの資産管理手順書・技術 | ネットワーク内の通信端末可視化と制御 | FortiNAC / OT-IDS | 予防 |
| | ルール策定・管理 | サイバーセキュリティ関連ルール・教育組込 | コンサルティング | | 予防 / 事故対応 |
| 技術（Technology） | 端末保護 | 工場システム端末のセキュリティ対策 | • クライアント保護と一元管理<br>• 仮想パッチの適用<br>• アプリケーションホワイトリストまたは指定通信の遮断<br>• おとり捜査によるアクティブディフェンス | FortiGate / FortiEDR / OT-IDS | 予防 / 事故対応 |
| | 物理 | 工場の物理セキュリティ対策実施 | 物理対策実施のこと(カメラ、入退館管理等) | FortiCamera | 予防 |
| | ネットワーク | 工場ネットワークのセキュリティ対策 | • VLANによるセグメンテーションとセキュリティ対策<br>• ネットワーク内の通信端末可視化と制御 | NAC / Deceptor / Gate / OT-IDS | 予防 / 事故対応 |
| | ログ | 工場のセキュリティログ取得・保存 | 通信ログの保存とレポート | FortiGate / FortiAnalyzer | 事故対応 |
| 工場資産サプライチェーン | 外部管理 | SI/ベンダーセキュリティ管理ルール | コンサルティング | | 予防 / 事故対応 |
| | 内部管理 | 工場資産調達時のセキュリティ管理ルール | コンサルティング | | 予防 |

# OTセキュリティコンサルティングラインアップ

松竹梅オプションによりリスクベースの優先順位付けと予算とのバランススタートが可能

| | 梅①：予防 Ver | 梅②：事故対応 Ver | 竹：”梅”+技術 | 松：“評価B”達成 |
|---|---|---|---|---|
| 詳細把握 | 詳細把握ヒアリング | | | |
| 組織 | ガバナンス体制 | | | |
| コンサルティング | 現場教育 | インシデント対応フロー<br>教育のみ | 現場教育 | |
| 運用 | | インシデント対応 | | |
| コンサルティング | ルール策定・管理 | OTセキュリティリスクと<br>脅威の入口のみ | ルール策定・管理 | |
| | | | | 資産管理 |
| | | | | 定期評価 |
| 技術 | | | 端末保護・ネットワーク・ログ | |
| コンサルティング | | | | 物理セキュリティ |
| SCM | | 外部管理（一部のみ） | 外部管理 | |
| コンサルティング | | | | 内部管理 |

# “サイバー事故調”制度の認知度向上に向けたフォーティネットの取り組み

## 事故調制度に関するメディア向け勉強会 (2024/4/10開催)

◆開催概要

重要インフラ防衛に向けた最新のサイバーセキュリティ関連法令改正の概説
ならびに日本のOTセキュリティ進捗状況

◆登壇者

名古屋工業大学：越島一郎 名誉教授

フォーティネットジャパン：佐々木、藤原

### 7件のメディア掲載

TECH.ASCII.jp 福澤記者 4/11
重要インフラの事故対応にサイバー視点を
― OTセキュリティ関連法改正をフォーティネットが解説
https://ascii.jp/elem/000/004/193/4193582/

ZDNet 國谷記者 4/12
OTのセキュリティでこれから必須になるインシデントへの対応
https://japan.zdnet.com/article/35217597/

マイナビTECH+ 今林記者 4/12
国家安全保障の観点から防衛が必要な重要インフラに必要なセキュリティ対策とは
https://news.mynavi.jp/techplus/article/20240412-2925452/

MONOist 長沢記者 4/16
OTセキュリティを巡るエネルギー業界の法改正とは、変わる事業者の事故対応
https://monoist.itmedia.co.jp/mn/articles/2404/16/news056.html

ITmedia エンタープライズ 宮田記者 4/16
OTセキュリティ関連法改正で何が変わる？ 改正のポイントと企業が今やるべきこと
https://www.itmedia.co.jp/enterprise/articles/2404/16/news025.html

週間BCN ニュース
フォーティネットジャパン、診断サービスの利用が拡大 法改正で求められるOTセキュリティーを強化
https://www.weeklybcn.com/journal/news/detail/20240425_203759.html

週間BCN 今日のヒトコトWeb版
https://www.weeklybcn.com/journal/column/detail/20240426_203864.html

## イベント出展による 概要説明・ソリューションコンセプト展示

2024/1/31 – 2024/2/2 IIFES2024 @東京ビッグサイト

**2024/1 @IIFES2024**

**2024/6 @Interop Tokyo24**

2024/6/12 – 2024/6/14 Interop Tokyo24 @幕張メッセ

**2024/10/30-11/1 @計測OSAKA2024 出展予定**

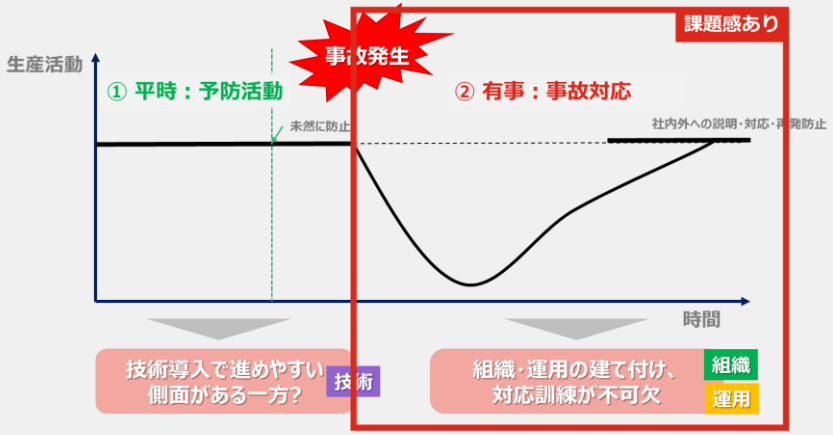
# まとめ

# 重要インフラ事業者の工場セキュリティ課題と対策

平時も、インシデント発生時も説明責任が求められる時代における打ち手とは

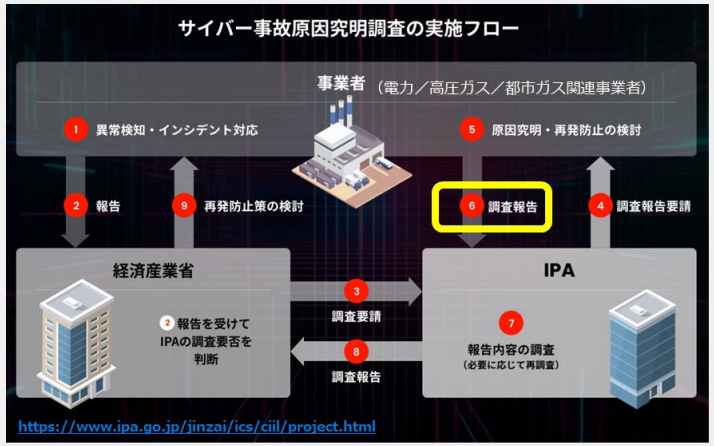
## 重要インフラ事業者の課題

- 今まで以上に**「説明責任」**が求められる中での**「実効性」**（＝効果的なリスク低減）との両立
- 万が一の**「事故対応」対策**：事業継続、コンティンジェンシープラン



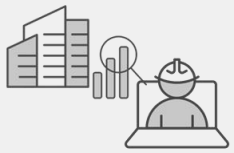

## サイバー事故調制度

- **エネルギー関係事業者が現在対象**。将来は？？




書面調査 → 十分に原因の究明が図られなかった場合 → 現地調査

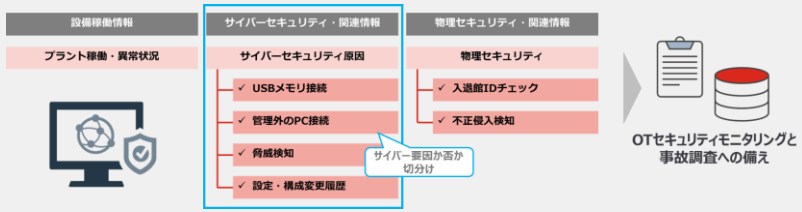
<報告書項目 *2>
1. システム構成
2. 情報セキュリティ管理体制
3. サイバー事故の概要、被害及び経緯
4. サイバー事故の技術的・組織的要因
5. 再発防止策（事業者考案）
6. 再発防止策への評価（必要に応じ、より適切な再発防止策を経産省が提言）



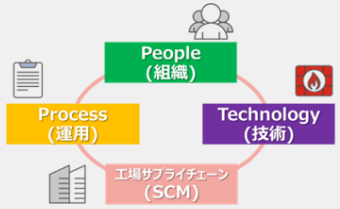
## 備えよ、事故調査！

事故調査に必要なもの
＝**ログ＆OTセキュリティ管理体制**

<ログ集約管理ソリューション>




<OTセキュリティ管理体制の構築支援>
（アセスメント／コンサルティング）




IPA立入調査への備えと事故対応体制構築

**フォーティネットは、OTセキュリティのリーディング企業として、制度啓発と対応ソリューション開発を推進します**

FORTINET

# OTセキュリティといえばフォーティネット