# 協働の会の活動目的と報告

「脅威を持続的に研究するWG」
大森 雅司

# 協働の会について

協働のいわれ；同じ目的のために、協力して働くこと。

**我らヤマトの民の末裔「お天道様と協に汗して働く喜び」**

①「協働の会」は、JNSA、IPA、JPCERT、JASAの4組織が連携し、同一方針の基に協働して、社会貢献の為に活動する事を目的とした集合体です。

②各種分野の欠けてる概念や不足している理解を相互補完し、サイバーセキュリティに関わる課題を全体として捉え直すことを狙いとします。

③考え方や構造・発想の異なる各種分野間の『橋渡し』を行います。

④複数に跨った分野間で『腹割って話し、相互理解の第一歩となる』場と機会を提供します。

⑤相関整理された「橋渡し材料や整理学」を、政府等関係各所等に情報発信し、実情を踏まえた実行可能性の高い政策立案等に示唆誘導することを目標とした活動を行います。

⑥情報交換会を開催し、各種課題を掘り下げた議論の場とします。

# 主要課題と活動内容A

JNSA

## A. サイバー攻撃と重要インフラ保安管理体制（保安事故防止体制）との関係整理⇒IIoT化、IoT国際標準化を視野

### ①重要インフラ分野各制御系システムの事業者ヒアリング

- 化学プラント、放送、電力、鉄道、航空、金融など
- 「システム形態、保安等管理体制、保安基準等」調査
- **サイバーと保安管理の関係を整理**


### ②攻撃モデルの机上トレースによるハザードシナリオ検討

サイバー攻撃の特性：

- サイバー攻撃は、機器故障、誤操作と同じ**引き金事象**の一つ
- サイバー攻撃は「**人工的に（意図を持って）**設備等の装置異常を**同時多発的に**引き起こす」現象と定義
- 「**攻撃難度の壁（意図性の壁）**」を組みこむ

STOP

攻撃難度の壁

独立防御層

装置障害発生以降は他事象と同じ既存保安管理対策で対処

保安事故（異常現象）

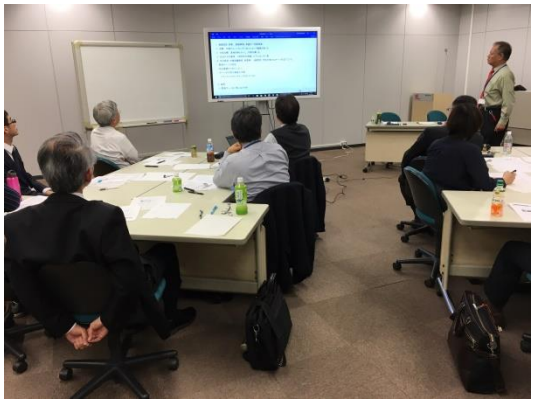
# 主要課題と活動内容B

## B. 事案段階(インシデント)から事態段階(アクシデント)に至った場合の組織パニック(エリートパニック)回避問題

### ①JASA「机上演習(TTX)指導員養成講座」の開催

- TTX指導員の養成(13名)を目的
- 本年度4月から1年間、講座を開設
- 来年度JASA会員への演習実施

TTX全体の流れを体験してみよう！
実際にシナリオを作ってみよう！
実例に基ずく組織パニックシナリオを作成！
蓄積したシナリオは「ノウハウ集」として教育等に利活用！



# 主要課題と活動内容C

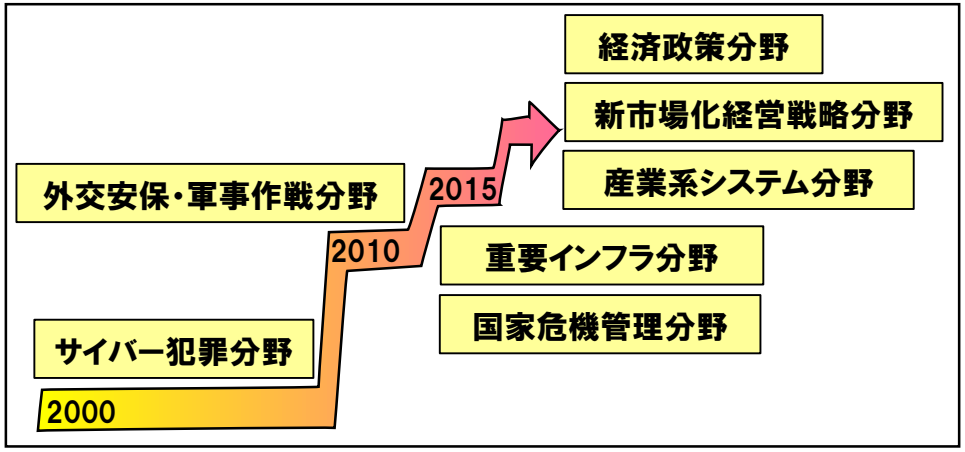
## C. サイバー問題全体象の関係理解、特に多様な意味を持つIoT問題の整理

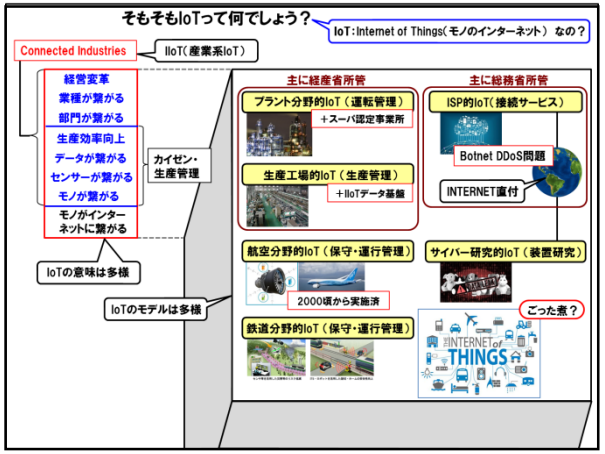
1. サイバー問題全体象の関係整理

IoT分類、IoT基盤、生産工場事例、IoTビジネストレンド、コネクティッドインダストリ、サプライチェーン問題と米英国際規格の動き、さらには、デュアルユースや武器輸出や一帯一路問題等、多様な分野との関係が生まれたサイバー問題全体象の関係を理解し全体象整理を行う。

2. IoTとConnected Industries

特に、製造業側でもIoTとIIoTという言葉が入り乱れ始めた今般、テーマキーワードをIoTのままでいいか、IoT分類的にはIIoTが示すコンセプトも分類対象にするのがいいのか？IoTとConnected Industriesドクトリンの関係、などのIIoTとIoTの概念整理が喫緊の課題。



# 第2回協働の会（2017/9/11）

**参加者集計**

協働の会；予定数226　参加数219　参加率97％

呑みガヤ ；予定数134　参加数121　参加率90％

**省庁等参加者；**

「NISC、警察庁、総務省、農水省、宮内庁、IT戦略室、厚労省、国交省、海保庁、法務省、自衛隊、衆議院事務局、JC3、IPA、JPCERT、産総研等」



# 第3回協働の会（ワイガヤ通算26回目）

## 日本の為に
## 人様の為に
## 「協働の会」

協働の会：228
呑みガヤ：122

# プログラム（情報交換項目）

JNSA

## テーマ①サイバー問題全体象の関係理解、特に多様な意味を持つIoT問題の整理

1.サイバーセキュリティのテーマの変遷と全体像：JNSA　岡谷

2.各分野の考えるIoTイメージの紹介とモデル整理

(1) プラント分野的IoT（IIoT）「運転管理」:三井化学　十河さん
「化学プラントのIoT化　～三井化学における先進技術活用事例紹介～」

(2) 生産工場的IoT 「生産管理・品質管理」:IPA　堀さん
「工場のIoT化とセキュリティリスク　～対策の在り方の現実論とは？～」

(3) 航空分野的IoT 「保守・運行管理」:ANA　→第４回協働の会（５月連休頃）で実施予定
「航空機の運航整備管理システムの現状とIoT化課題（仮）」

(4) 通信事業者的IoT 「接続サービス、データプラットフォーム」:NTTcom IoT推進室　宮川さん
「IoTセキュリティ視点から見た通信事業基盤」

(5) サイバー研究的IoT 「学生教育、装置解析、模擬攻撃」
九州大学　小出先生 「研究者及び教育機関から見たIoT、ProSec（enPiT-Pro）紹介」
三菱電気　木藤さん 「IoT機器のリバースエジニアリング動向、解析デモ等」

(6) 医療分野のIoT 「IMoT」:保険医療福祉情報システム工業会（JAHIS） 茗原さん
「医療IoTにおける安全管理とセキュリティ」

(7) IoTインシデントレスポンスの実例：JPCERT　佐々木さん
「Wannacry亜種感染、ブロードバンドルーターMirai亜種感染、IoT機器へのグローバルIP付与問題等」

(8) グローバル視点でのIoT：GE　トリワイさん
「欧米等グローバル市場における各分野のIoTモデル（鉄道分野的IoT含む）」

(9) 各IoTの運用特性を踏まえたモデル化整理　岡谷

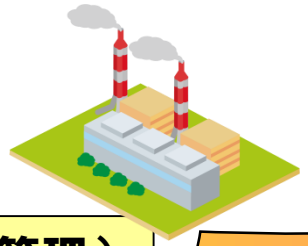
JNSA


自衛隊元最高幹部
が教える
経営学では学べない戦略の本質
折木良一
「きれいな戦略」だけでは、人も組織も絶対に動かない
「原発事故と戦い抜いた究極のリアリズムを体感せよ」
野中郁次郎氏絶賛!
「シン・ゴジラ」自衛隊トップのモデルとされる伝説の自衛官がここまで軌道を明かした!
KADOKAWA

# サイバー問題の背景や課題

# サイバー問題が関わる分野の増加とそれぞれの意図

「産業系セキュリティ分野」



重要インフラ分野（危機管理）

国家危機管理分野

外交安保・軍事作戦分野

サイバー犯罪分野

2000

2010

2015

2017

経済対策関連政策分野

新市場化経営戦略分野

産業系システム分野

重要インフラ分野（市場化）

産業系の仮想脅威

第4次産業革命
Society 5.0
未来投資戦略2017
Connected Industries
IoT（IIoT=産業IoT）
グローバル市場IGT

外交ツール・軍事工作戦術

実犯罪の増加

JNSA

# 各分野の実情を踏まえた現場調査（と整理学の分析）

# 各分野の考えるIoTイメージの紹介とIoTモデルの整理

そもそもIoTって何でしょう？

IoT：Internet of Things（モノのインターネット） なの？

Connected Industries

IIoT（産業系IoT）

経営変革
業種が繋がる
部門が繋がる

生産効率向上
データが繋がる
センサーが繋がる
モノが繋がる

カイゼン・
生産管理

モノがインターネットに繋がる

IoTの意味は多様

IoTのモデルは多様

## 主に経産省他の所管

### プラント分野的IoT（運転管理）

＋スーパ認定事業所

### 生産工場的IoT（生産管理）

＋IIoTデータ基盤

### 航空分野的IoT（保守・運行管理）

2000頃から実施済

### 鉄道分野的IoT（保守・運行管理）

センサ等を活用した災害等のリスク低減

ITS・ロボットを活用した踏切・ホームの安全性向上

## 主に総務省所管

### ISP的IoT（接続サービス）

Botnet DDoS問題

INTERNET直付

### サイバー研究的IoT（装置研究）


ごった煮の図？


そもそも、IoTやOTは…米発信で…IT分野業界が言い始めた造語であり、その真意は「産業系分野にITを展開したい？」

# 「モノのインターネット」以外に多様な意味を持つ「IoT」

それぞれ、同じものを見てるようで別な事を考えてる！

分野によって異なるIoTの意味を考慮して会話することが重要

**製造IoT、IoT基盤**　生産性・品質向上

保安管理優先　ラインタイム優先

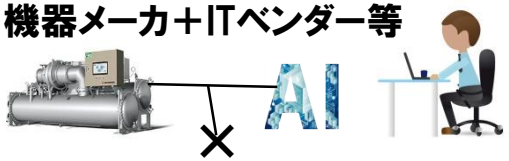
計装システム等　生産ライン系等

**運行・整備性向上**　**？？IoT**

人命優先
（運航安全・整備管理）


**IoT技術（+AI）**　見える化、故障予測

機器メーカ＋ITベンダー等



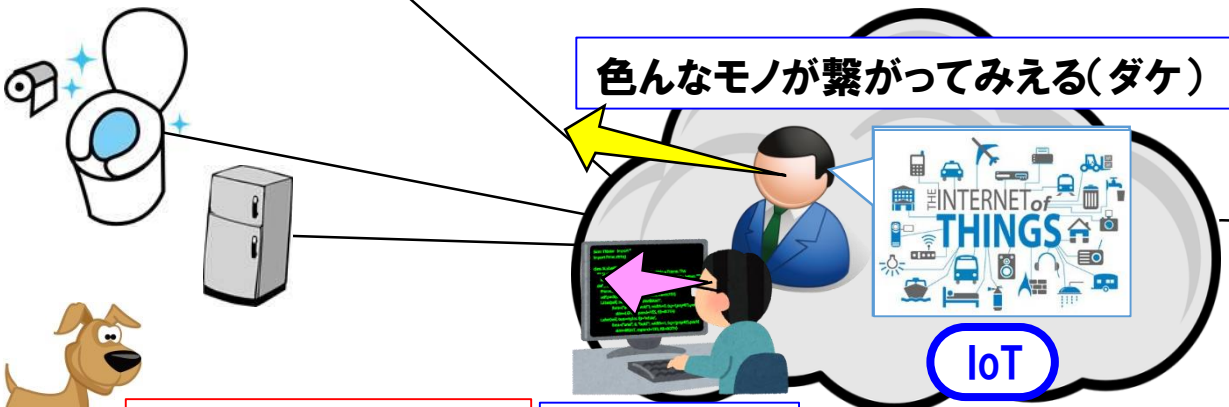

**医療IoT**　高度医療

人命優先
（医療安全管理）

遠隔医療

地方医師不足等

色んなモノが繋がってみえる（ダケ）




脆弱性と機器単体へのサイバー攻撃をゴールに

脆弱性発見 ⇒ 脆弱性対策のみでは過剰品質に走りがち！
保安管理や生産性確保との全体バランスを見落としがち

まとめ！

# サイバー攻撃と保安管理の関係

これらは様々な事業者（航空、鉄道、プラント、放送、生産工場等）の保安管理部門と意見交換した結果の整理学です。

既存の保安等体制で保安事故を防止
→サイバー攻撃＝保安事故ではない！

保安対策のリスク（医療安全管理に該当）

既存の事象対処と同じ
（応急処置→緊急復旧等）

①事故を起こさない→安全第一


保安事故の発生

保安管理体制の起動
（防災体制）


保安事象の発生
（安全停止←安全計装）

既存の保安等体制の存在

機器障害の発生

保安管理、医療安全、航空安全、鉄道案など
→国民の生命財産への影響が出る、保安等事故に関連する分野はほぼ同じアプローチ

サイバーリスク

引き金事象

②生産機会損失の低減→品質第二、生産第三

保安管理全体におけるサイバー攻撃の位置付けは「引き金事象」

サイバー対処は②生産機会の損失の範囲で過剰品質にならないようにバランスを考えて対処すれば良い！

- ポカミス、操作ミス等人的エラー
- 機器不具合（整備不良、さび等による動作不良等）
- 地震等災害
- サイバー攻撃による機器障害の意図的生起
  →これ自体が難しいが…

サイバー攻撃のみ特別に考えると過剰品質になる事もある。全体のバランスが大事！

# サイバー攻撃と既存の保安管理との関係に関する「２種類の整理学アプローチ」

まとめ！

JNSA

パターン①
サイバー攻撃を他の保安管理の引き金事象の一つと捉えるアプローチ
（保安管理分野はこの捉え方が多い）

サイバーセキュリティに関する体制、基準等
サイバーリスク

必要なのは、引き金事象対策の範囲内で、過剰品質にならない「サーバリスク対策！」

各分野既存の保安管理体制、各業法、安全規格等

保安管理上のリスク

保安事故の発生

パターン②
他の保安管理と同列単独にサイバー攻撃を捉えしまうアプローチ
（一般的に、ITサイバー分野はこの捉え方が多い）
→サイバー攻撃と保安事故発生に至る関係が整理できない
→既存の安全規格等との整合が取れない（既存の安全管理体制を壊さない事）

？

サイバーセキュリティに関する体制、基準等
サイバーリスク

？

JASAと協働し、問題検証型机上演習講座を開催

# 問題検証型机上演習（TTX）とは

ビジネススクールなどでは「**オリエンテーション**」と言いますが、手法は同じです。

**汎用的な「問題解決技法」の一種であり、ビジネス課題に対しても用いられる。**

- **問題事例の収集分析**
- **演習シナリオの作成**
- **演習の進行を制御**
- **検討結果の記録と再利用**

**技能演習ではなく、組織体制等の検証を目的とし、実態に則したシナリオを用いて行う危機管理型演習**
**→問題点を洗い出し、計画等に反映するのが目的**

**あえて問題課題にぶつかるように誘導し、考えさせるのが目的。**
**TTXの成否はファシリテータの能力にかかっている！**

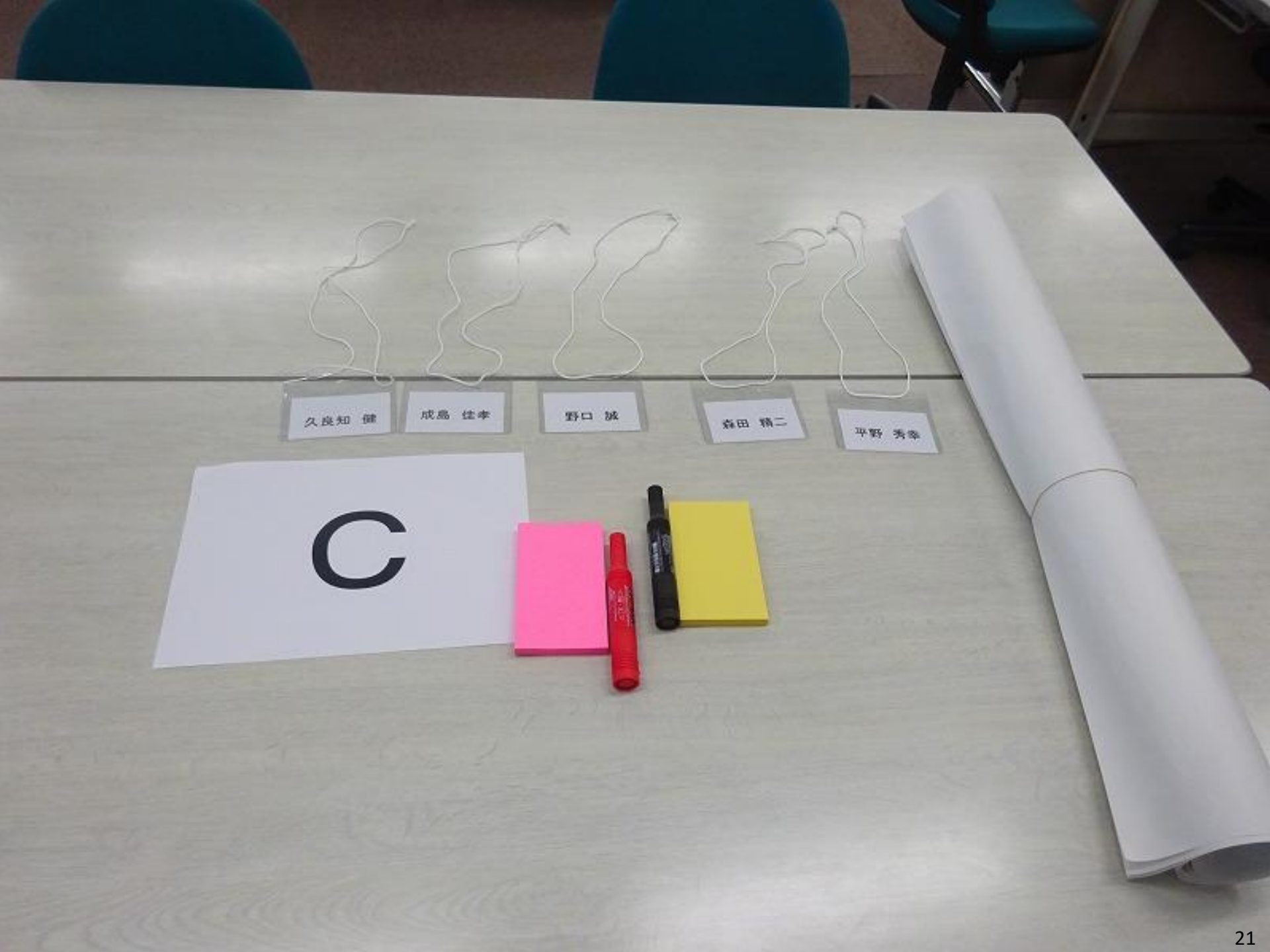
**シナリオに教訓を反映することにより、模擬体験による教育効果を得ることも可**

**様々な組織ノウハウを結晶させ保存する一つの形**

**狙いの違い**

**教育：知識を学ぶだけなので考えない　➡ マス生産向け**
**訓練：反復練習により能力を維持する　➡ ルーティン能力維持**
**演習：①自ら考え模擬体験して身につける ➡ 指導者育成向け**
**②組織の体制能力の検証　➡ 組織体制整備**

**軍の演習分類：参考**
- **総合演習**
- **機能演習**
- **FTX（実働演習）**
- **CPX（指揮所演習）**
- **TTX（机上演習）**


久良知 健
成島 佳孝
野口 誠
森田 精二
平野 秀幸
C

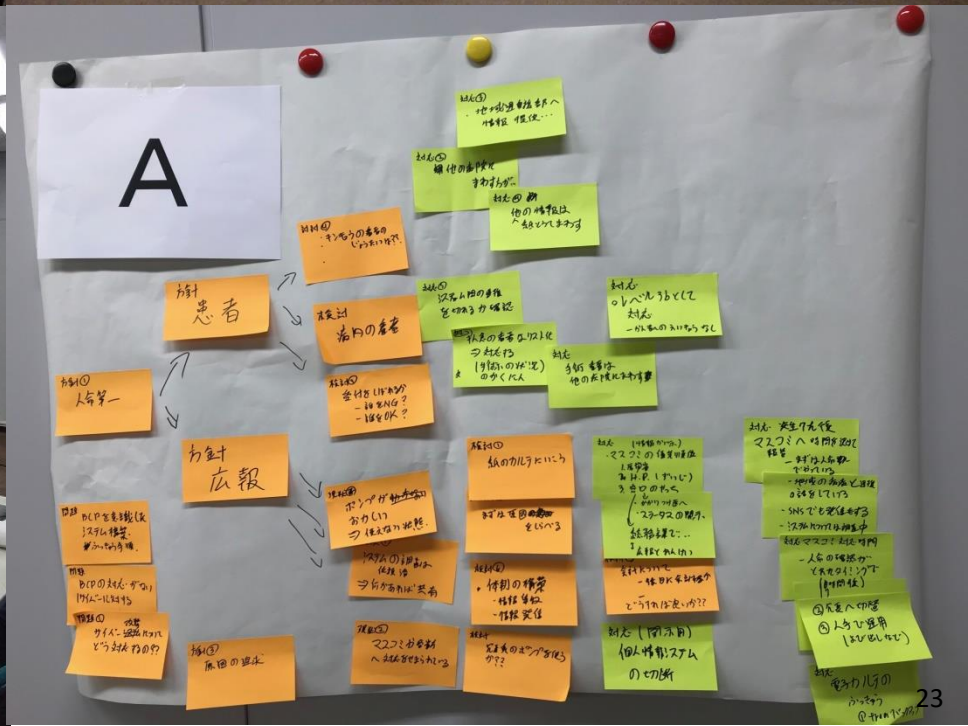
場面：医療安全管理委員会設置

ファシリテータ（状況付与と議論コントロール）


JASA
JAPAN INFORMATION SECURITY AUDIT ASSOCIATION
特定非営利活動法人 日本セキュリティ監査協会

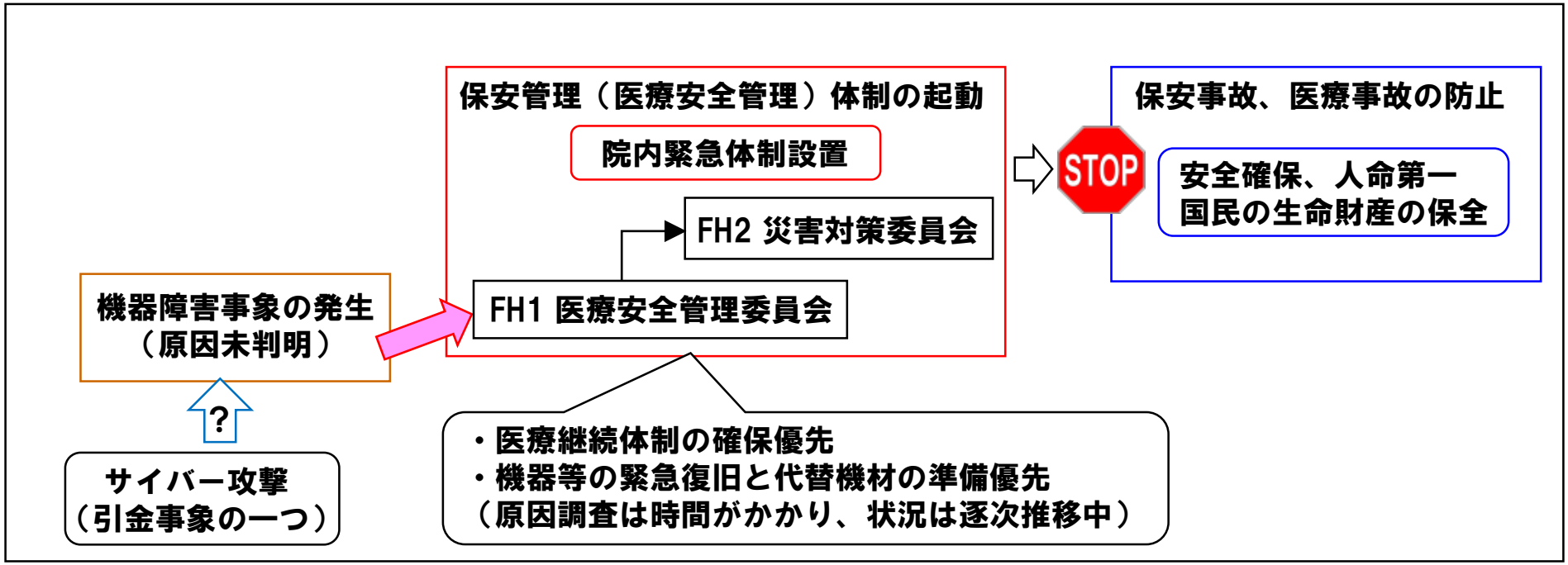
2017年度 第1回
サイバーセキュリティ机上演習ワークショップ レポート
2018年1月26日

http://www.jasa.jp/seminar/workshop_exercise_report.html?type=workshop_exercise_report


A
方針 患者
検討 病院の患者
方針① 人命第一
方針 広報

# JASA TTXにおける事態遷移プロセス（演習検証結果）

- 関係者は事態スタート（サイバー原因不明）で共通認識
- 病院は危機管理型組織であるため、組織パニック（エリートパニック）は発生しない
- 部外組織等（省庁、報道）側に組織パニックが発生
- 原因調査は再発防止の為であり、事態終息後に実施事態段階で必要なのはサイバーインシデントレスポンスによる回復ではなく、安全対処の為の応急処置。




- 医療安全分野も、他の重要インフラ分野における「サイバー攻撃と保安管理体制」の考え方と同じ。
- サイバー攻撃が直ちに命に関わる医療事故に繋がる可能性は低い（医療安全管理体制に移行）
- サイバー攻撃は機器障害に繋がるまでの現象
- サイバーインシデントレスポンスは、事態対処の概念ではなく事案対処の概念。

公益社団法人　日本医業経営コンサルタント協会（JAHIS）と協働し、「サイバーセキュリティ演習研究会」を設置。
本年度、医療安全管理分野のTTXを実施。

協働の会では諸課題に興味があり話を聞いてみたいという人（チーム）には、解説やミニ勉強会を行っています。

ご興味がありましたら、お声掛けください。