サイバーセキュリティ演習 WG　活動報告書

2018 年 3 月

日本セキュリティ監査協会

サイバーセキュリティ演習 WG

目次

内容

はじめに

本活動の目的

サイバーセキュリティ演習 WG（以降本 WG）は、TTX（机上演習）などを通して、今後重要インフラでも起こりうるサイバーリスクや組織パニック等のテーマを取り上げながら技術的な支援はもとより、経営層に対しても全体を俯瞰した適切な提言が出来る人材（橋渡し人材）の育成を目標としています。

組織パニックに備えて

昨今、年金機構情の個人報漏洩事案にみられるように、サイバーセキュリティの重大事案では、組織パニックが生じることがあります。組織パニックが起こってしまうと、本来の対策に注力できず、全ての対応が後手に回るおそれが生じます。組織パニックの原因は、インシデントが生じたときに見られる不完全で多様な情報と要求が、多方面から大量にかつ五月雨式に流れ込むことで、経営層が冷静さを欠いてしまうことにあります。組織の方向性が原因の究明や責任の回避に偏重することにより、本来の業務が停滞すると場合によっては、国民の生命や財産を脅かすより二次被害にまで事態は深刻化することもあり得ます。

このような事態を避ける為、サイバーセキュリティ担当者がリスクを分析し、経営層に全体を俯瞰した適切なアドバイスができるようにするための思考訓練として TTX（机上演習）が適しています。また、実際に発生した事象・事件をシナリオとして掘り起こしシュミレーションすることで新たな課題、より最適な改善策を導き出すことがあります。本 WG は CIO 補佐官から、情報セキュリティ監査人、コンサルタント、エンジニアまで様々な背景を持つメンバが集まってお互いの暗黙知を提供しあい、お客様の深刻な事態案件（アクシデント）を収束に導くレジリエンス型のシナリオを検討してまいりました。

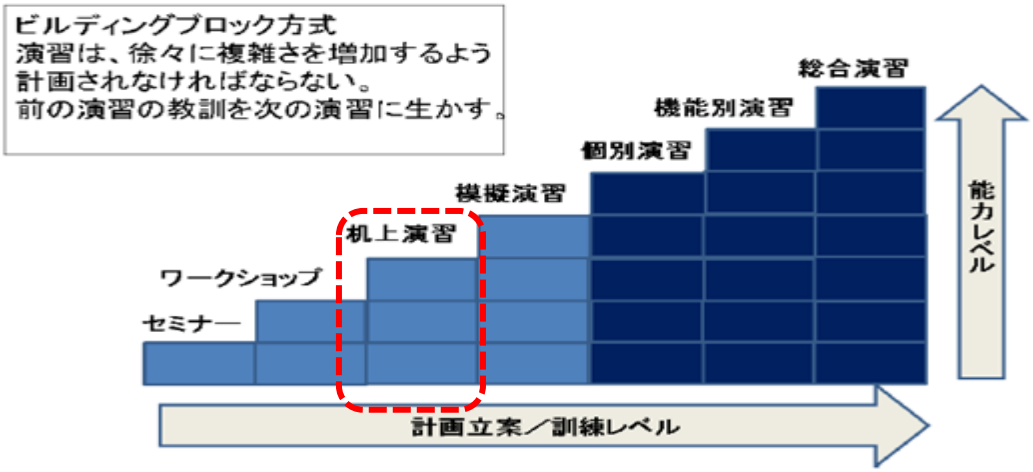
実際に作成したシナリオで演習を実施すると進行役（ファシリエータ）と参加者（プレイヤ）が互いに多くの気づき、学びを見出すことが出来ました。

組織パニックに備えて、我々は経営層に対して答えがない経営判断をせざるを得ない時でも事業の継続を主軸において技術と組織運営の両輪が滞りなくまわるようなしなやかで強靭な組織へと導く道標となるよう、演習企画技官としてのファシリテータの養成に注力していきます。

１．　TTX（机上演習）とは？

TTX とは、想定かつ模擬した緊急事態の様々な問題に関する議論を引き起こします。
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であり、問題点洗い出し、計画等に反映するのが目的です。

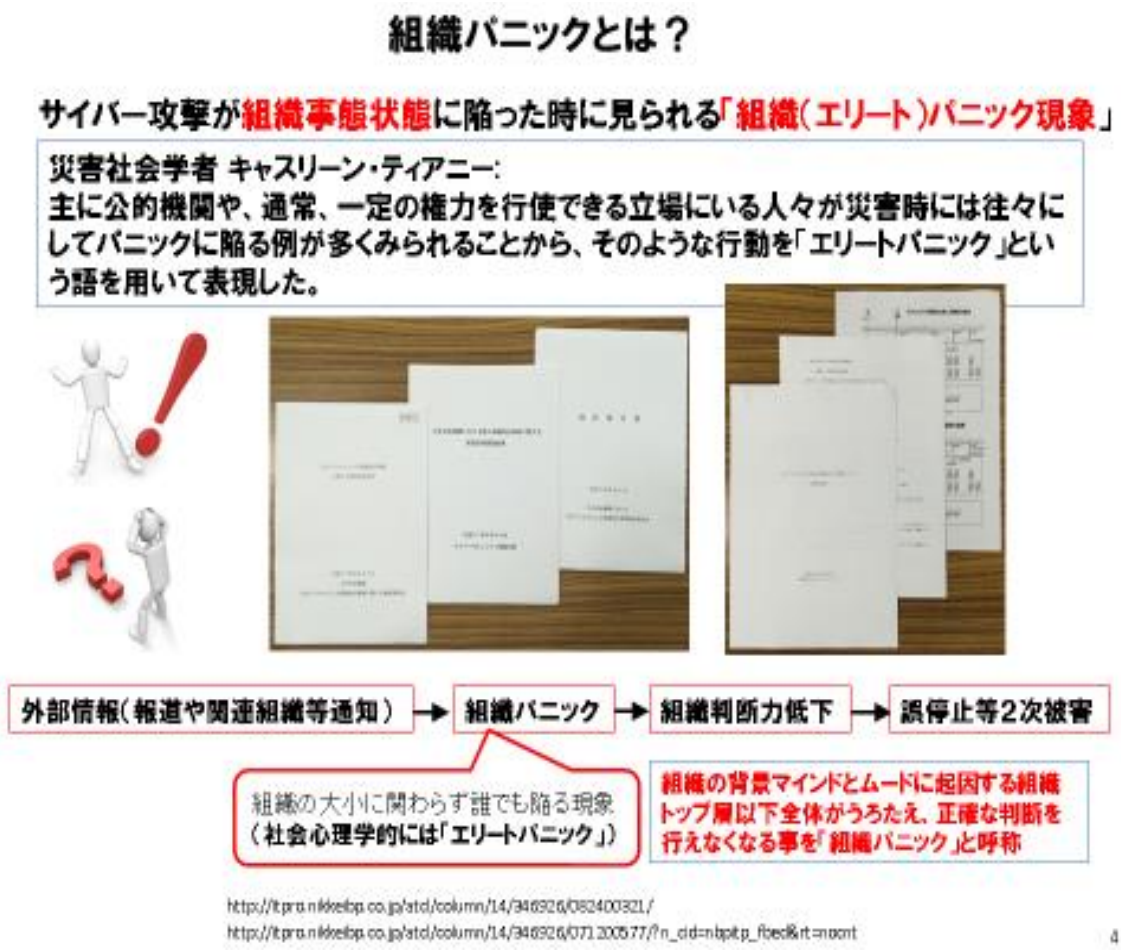
出典　日本コンサルティング推進機構　専門コラム「指揮官の決断」 図上演習の秘密
https://www.jcpo.jp/archives/19784



机上演習の位置づけ

出典　株式会社　ラック　　公益財団法人　防衛基盤整備協会
情報セキュリティの現状と動向について―サイバー演習の実施要領と演習事例―
https://ssl.bsk-z.or.jp/kakusyu/pdf/27-1jyouhousekyurithityousakennkyuu.pdf
演習には分類があり、演習のレベルが上がるほど計画立案の要求レベルも広範囲/複雑になり演習そのものも大規模になります。

２．　組織パニックとは？



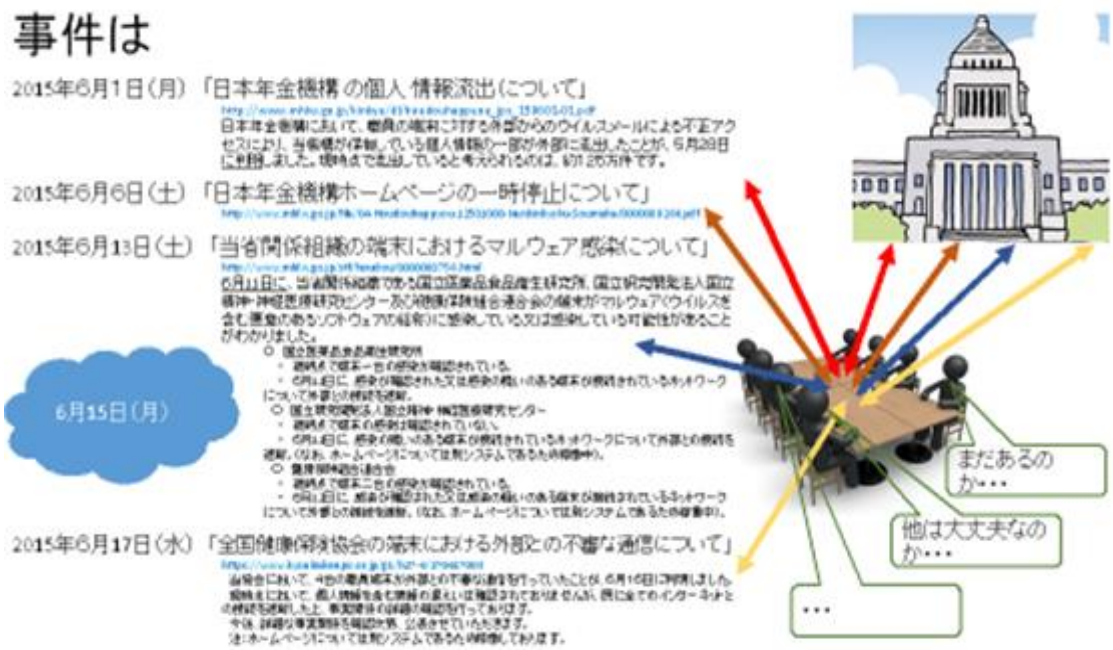
組織パニックとは、社会心理学でいわれるエリートパニックを組織全体の事象として置き換えた造語になります。一般人のパニック状態とは違い、組織の中枢でより強い影響力を持つエリート（経営層）がパニック（自己保身による回避行動、逃走、隠蔽）に陥ると、組織全体での判断力が低下しより広範囲に二次被害を引き起こす可能性が高くなります。

国民の生命や財産にかかわる重要インフラ（ライフライン、金融、社会保障、医療など）で発生すると被害は甚大かつ深刻になります。組織全体がパニックになると本来のミッションを見失い、安易なリスク回避や、原因調査といった手段が目的になり、結果感染拡大防止を免罪符に正常に機能している業務システムや全ネットワーク遮断し機能停止に巻き込こもうとします。

組織パニックを回避するためには、事象としての組織パニックと向き合い、発生する仕組みを検証し、理解する必要があります。

３．　組織パニック事例

組織パニックの一例として「実ビジネスや業務の影響を考えずに何でも止めればいい、ネットワークを遮断すればいいと考えるエリート達」の存在があります。以下は日本年金機構の事例になります。



メンバーが**役職者**ばかりで、実動要員が不在

- インシデント（であるかどうか）の判断は現場任せ
- 部下からサポートを受けないと行動をとれない
- 情報通信技術（IT/ICT）の教養と経験が不足（適切な指示が出せない）
- 責任追及に偏重しがち（“責任者が責任者を探す”）

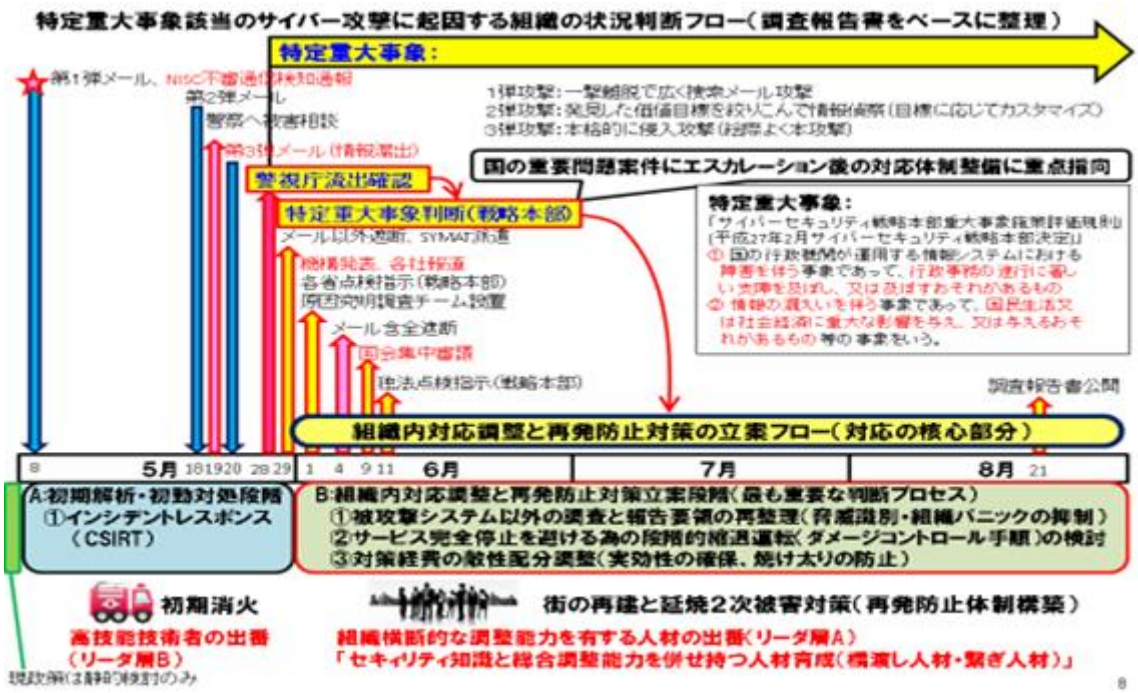
適切な**状況認識**ができていない

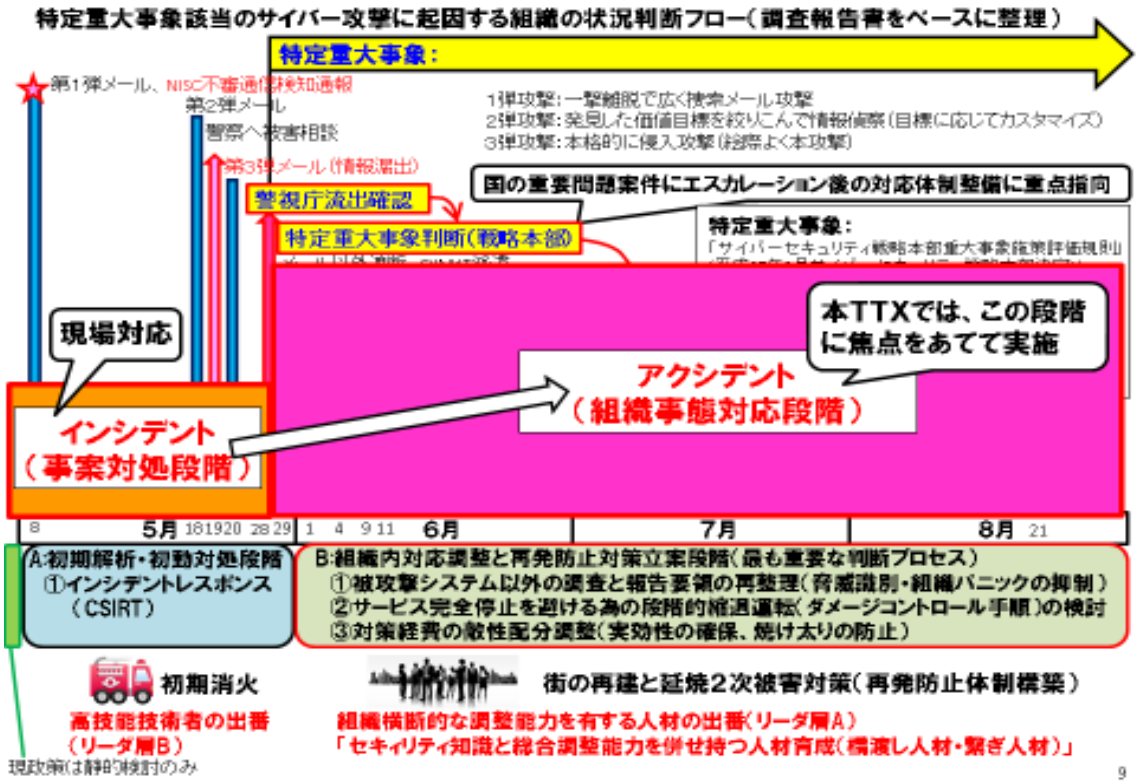
- 関連情報として入手するものが日本語のみ
- 外部のチーム（組織）とのコミュニティケーションができていない
- 専門技術用語を伴う報告から全体像を把握することが難しい
- 顕在化した情報のみで認識しようとする傾向が強い
  （潜在化した可能性のある事実への追求姿勢が見当たらない）

下段　出典　なぜ、日本のインシデント対応能力は向上しないのか

名和　利男　2017 年 2 月　寄稿

４．　組織パニックの対象範囲

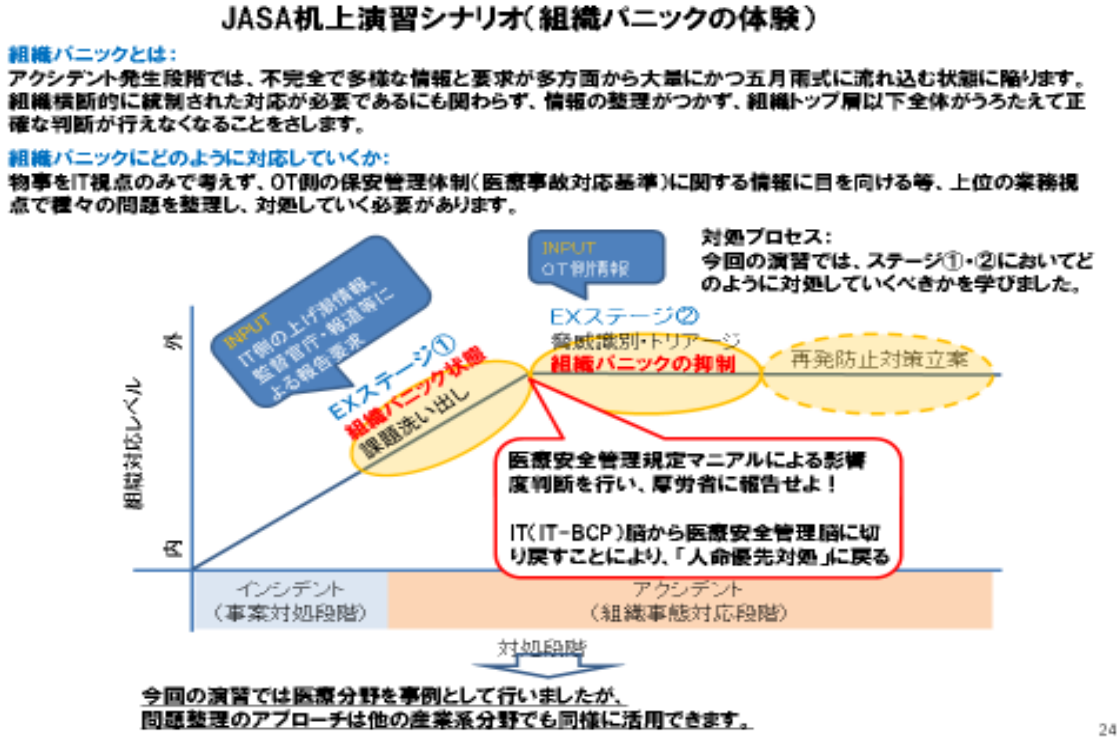




出典　サイバー問題の全体像と本質を見に行く　岡谷　貢　2018 年 2 月　講演資料より

直面しているのはインシデントの範囲を超えています。アクシデントであることを受け止めなくてはいけません。

５．　JASA 机上演習シナリオとは？



本 WG ではシナリオ作りにおいて場面の設定に多くの検討を要しました。
以下に場面設定の方向性に関する考え方をご紹介します。

本シナリオは、組織パニックに陥った組織を優秀なインシデント対応部隊がサイバー攻撃の原因を調査してマルウエアなどを特定、システム復旧してパッチ適用して一件落着といったインシデント対応のシナリオではありません。

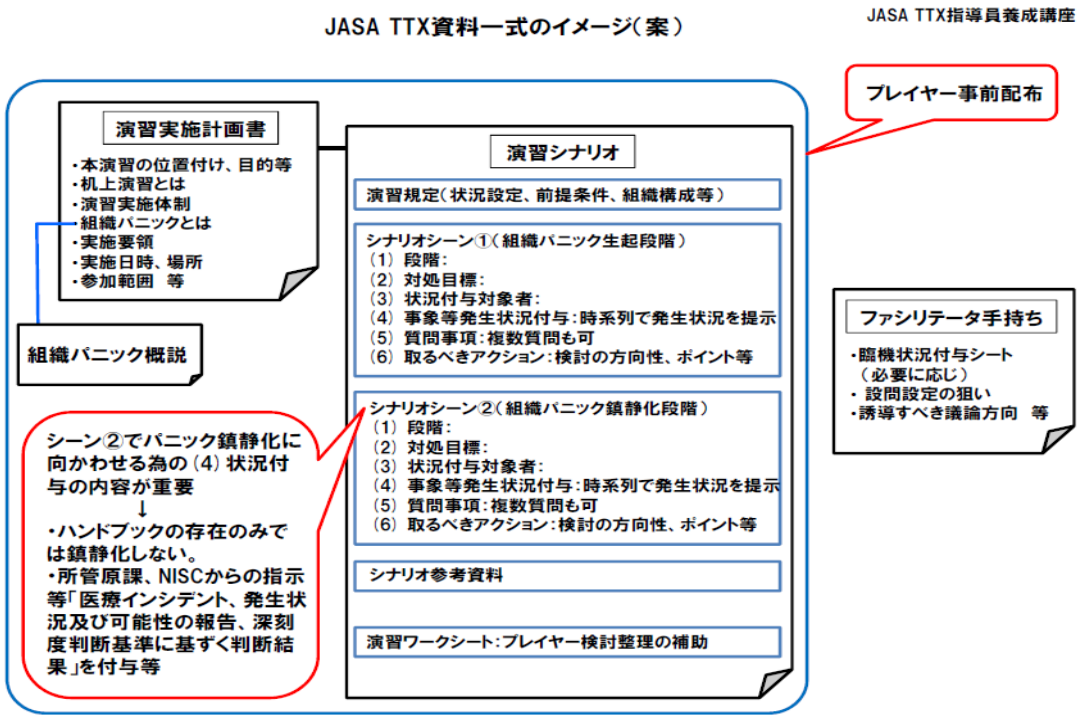
今回は時系列を無視せず、リアルタイム型の演習として組織内に噴出したリスクを洗い出し、対処の優先順位を決め、タスクフォースに体制を移行、ダメージコントロールしながら業務継続させることを想定しています。いわば組織パニックに耐性がある強靭な組織作りの為のレジリエンスタイプシナリオの実践です。よってサイバー攻撃自体は単に引き金事象にすぎないことを理解しなければいけません。

当初は、組織パニックに陥ったプレイヤ（登場人物）の紛糾の矛先を医療システムのシステム担当部長を想定しました。しかしパニック状態からダメージコントロールフェイスに移行するトリガーを弾く役目は組織全体に影響力を持つ副委員長（経営実務を掌握）を巻き込む必要があるため、検討の末矛先を変更しました。むしろシステム担当部長は状況を適切に把握し、助言を与える存在で良いのです。

さらにプレイヤに医療安全管理規定といった業務指針に目を向けさせることで問題の焦点をサイバー攻撃への対応ではなく、本来の医療機関としてのトリアージを実施出来るように仕向けました。

シナリオには起承転結が必要であり、起だけでは演習が停滞してしまいます。誰が承り、何が転になるかさえ決まれば結は自ずと導き出されます。このような経緯をもって EX ステージ１（課題洗い出し）と EX ステージ２（脅威識別・トリアージ）の骨格が整理されました。

6．　JASA　TTX 資料一式イメージ



以下に JASA　TTX 資料一式の構成を紹介します。

① 演習実施計画書

② 演習シナリオ

③ ファシリテータ手持ち資料

① 演習実施計画書（プレイヤに事前配布）

いわゆる開催案内です。演習の目的、実施体制、実施要項など本演習の実施あたって必要な情報を記載します。演習が終れば振り返りや改善提案として別途報告書も必要になります。

② 演習シナリオ（プレイヤに事前配布）

シナリオの本体です。メインはあくまでプレイヤによる演習の為、必要な情報はあらかじめ配布しておきます。セミナー形式といった異業種間で実施する場合はある程度リアルな世界観の設定が必要です。

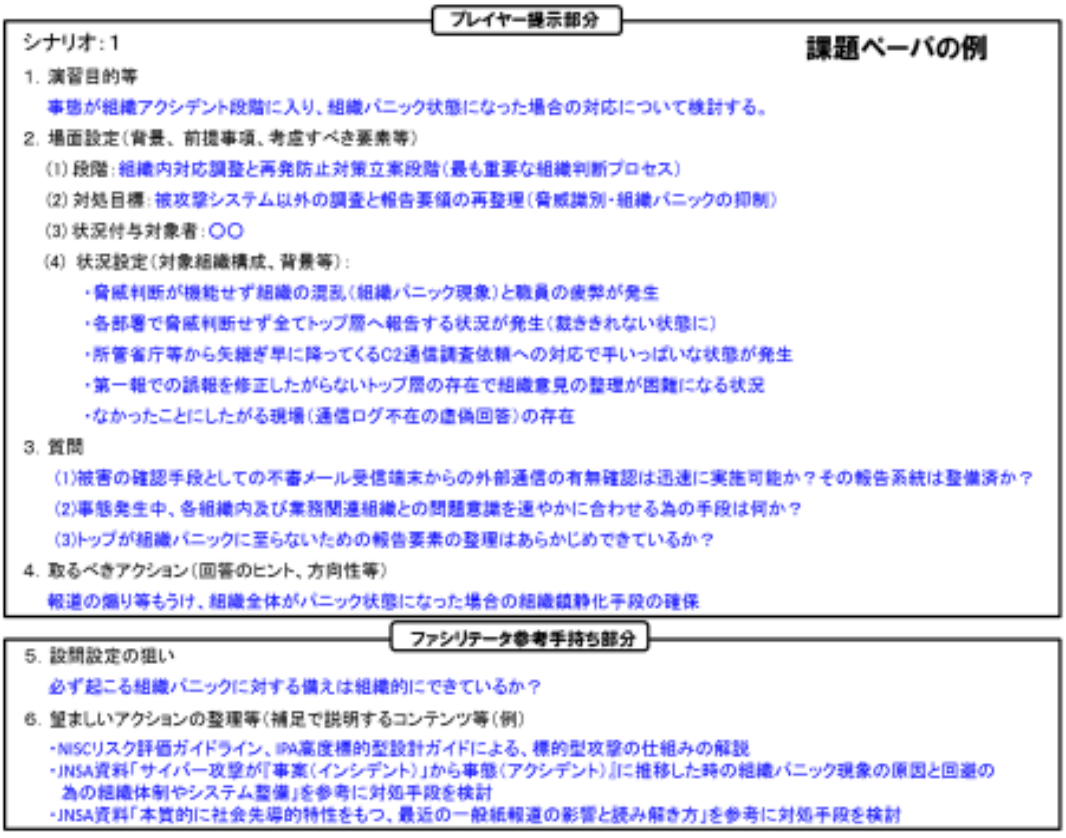
例として標準的な病院のプロフィール、内部環境/外部環境情報、連携部門、業界の最新動向など。

重要なのは演習に「タラレバ」が起きて議論を発散させないように制約を与えることです。そのためシナリオは**実際に起きた事象の公開情報をベースにシナリオを作成、補完することが望ましいです。**

③ 進行役（ファシリテータ）手持ち資料（配布を行わない）

進行役にとってのメモであり、サプライズで新たな条件付与を行う場合の備忘録や演習目標の評価簿に使います。また、演習では進行役の狙いとかけ離れたプレイヤ側での議論の発散、脱線、停滞が発生します。進行役は演習目標に沿った議論に軌道修正する必要があるため、事前に FAQ や想定問答を整理しておくと良いでしょう。

７．　課題シナリオ例



課題シナリオの例になります。例の内容は情報システム部門がターゲットになり、各方面から問いあわせが殺到しシステム部門が機能不全に陥る事を想定しています。

ここで疑問になるのが組織パニックという言葉の定義をどこまで解釈しているかという点になります。

パニックになっているのは機能不全に陥ったシステム部門の担当者個人だけではありません。パニックになっているのは経営層（エリート）の責任の回避行動、情報の隠蔽を決め込む現場など組織全体にまたがります。

ネットや SNS に書き込まれた内容を確認するために詰めかける報道陣や利害関係にある関係部門も含めてパニックとみなす必要があります。システム担当者だけに限れば単に個人レベルの許容量だけの話であって、インシデント対応と同様責任分界の範囲で土竜叩きをしていればいいだけの話です。

プレイヤがブレインストーミングした内容に対して、進行役（ファシリエータ）はプレイヤが組織パニックを想定した備えが充分できているかどうかを進行中にチェックします。足りない部分があれば望ましいアクションの整理で補足となりうるコンテンツ（ガイドライン等）を紹介します。

もしプレイヤの議論の中で調査の為にシステムを全停止するといった内容がでた場合はその影響範囲や実現性、有効性について議論させてみると良いでしょう。

８．　プレイヤ（配役）のアサインと場面設定

プレイヤ（配役）のアサインと場面設定の考え方

演習の実施にあたり、班（グループ）単位の適正な人数は４人から６人が妥当とされています。それ以上だと議論が発散する可能性が高いからです。１名は議事係として必要になるのでそれ以外は組織パニックに巻き込まれやすい現場の管理部門と決裁権を持つ経営側の実務担当にアサインします。

今回は医療現場を舞台として設定しているので医療関係者を例にとります。

・副医院長　病院経営の実権を任されています。安全管理委員会の責任者です。

・システム担当部長　各種医療情報システム及び機器ベンダーとのパイプ役です。

・看護部長　患者のケアなどを総括し現場視点で患者側の訴えを代弁します。

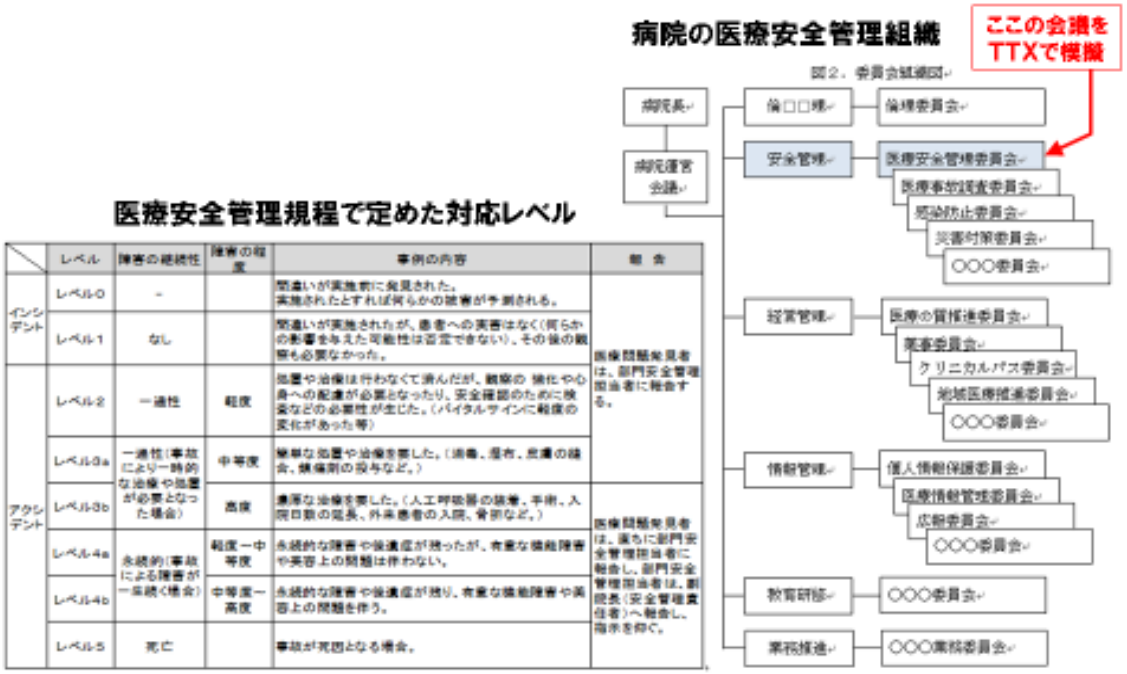
・診療部長　病院における現場医師達を総括する立場で医師達の訴えを代弁します。

・事務部長　医療事務を総括している為事務処理上の問題を訴えます。

・その他　人数に応じてアサインされてない役を割り振ります。外部とのパイプになる広報が最適です。急遽招集されたサイバーセキュリティやリスクマネジメントの専門家などオリジナル配役も可能です。入院中の患者、手術中の患者の親族などは緊急事態を演出する役として最適かもしれません。一時的に発生する、条件付与を与える役割はファシリテータ（進行役）が兼務すると良いでしょう。

（パニック状態の病院長、ベンダーSE、所轄官庁、マスコミ、政府関連団体）

９．　医療安全管理規定と安全管理組織



28

医療安全管理規定と安全管理委員会について

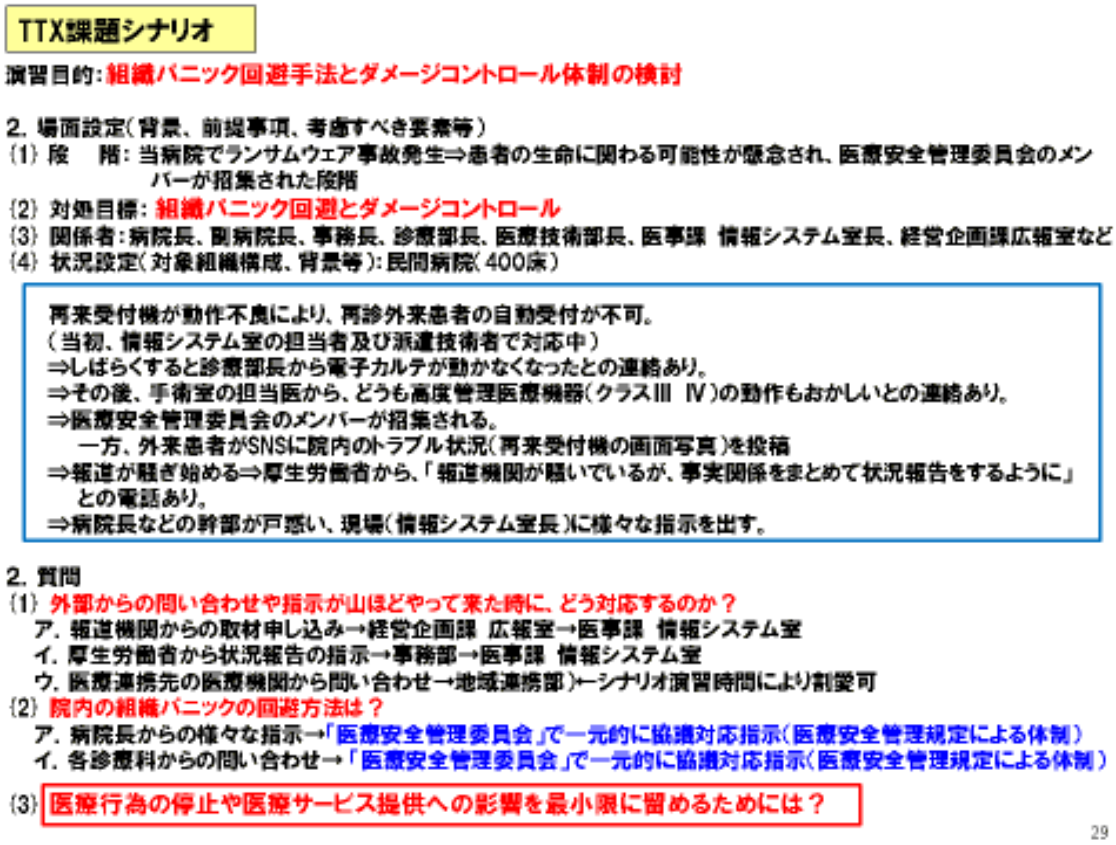
　シナリオを用意する上で、舞台となる組織の体制図、業務影響判断基準、対応フロー等に該当するアイテムが必要です。また、TTX の舞台は組織体制図上のどのような役割を持つ会議体であるかを示すことは TTX を円滑に進める上で重要です。今回は副医院長が責任者として開催する安全管理委員会が舞台となります。

　医療の現場では救急需要が同時多発で起きる戦争や災害では医療資源を効率的に配分し、最大多数の人命を救うことを目指すトリアージという考え方があります。最近では CERT によるインシデントレスポンスでも使われていいますが医療分野こそが元祖です。患者の重症度に基づいて、治療の優先度を決定して選別を行うことですがその考え方は危機管理下の組織運営にも適用できます。

　今回の医療安全管理規定は、医療現場がサイバー攻撃に振り回されず、本来の業務視点に立ち戻るための重要なアイテムとして使用します。

医療にかかわらず、人の命にかかわる重要インフラに携わる業界は、業種に拘らず厳格な管理規格を満たした多重独立防御層を形成しているため、情報システムが機能不全に陥ったくらいでは組織パニックにはなりません。それでも医療現場では想定外の事態をスイスチーズモデルやスノーボールモデルとなぞらえて日々訓練をしています。これは責任者が責任者を探す IT 視点の脆弱性との決定的な違いになります。

１０．　TTX 演習実施計画書



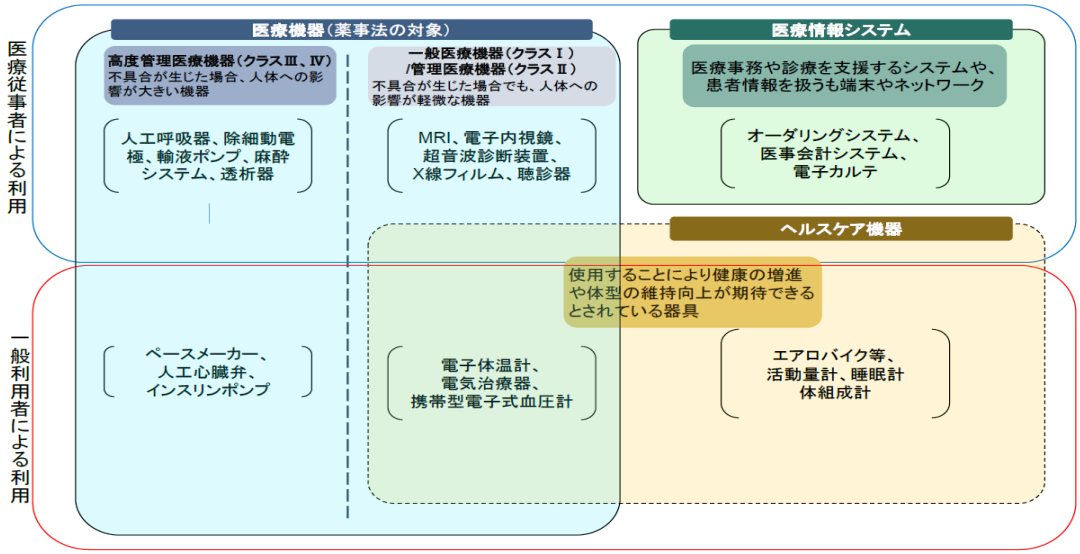
今回の医療シナリオを雛形に落とし込むと舞台の骨格が見えてきます。安全管理委員会は、院内、院外からの問合せに対して課題の洗い出し、より具体的な対応計画を立案します。
もちろん計画を実行に移すためのタスクフォースが必要です。これは職制を通した影響力のある権限を巻き込む必要あります。必要であれば権限を委譲し、外部執行機関を活用する場合もあります。
この時引き金事象であるサイバー攻撃によるシステム系の障害にひきずられないかがポイントになります。

大まかなシナリオの流れが決まっていれば細かなプレイヤー（登場人物）の入れ替えは演習グループ内で調整しても問題はありません。演習が発散、停滞するような場合は、進行役は、最後の手段としては議論を中断し、振り返りの時間や新たな条件付与などを追加して軌道修正を行います。

１１．　薬事上の医療機器の制約

型式証明を取得する医療機器

（利用者が勝手に改造修理を行ってはいけない）⇒利用者によるパッチ適用不可



出典　医療機器における情報セキュリティに関する調査（2013）（海外事例）

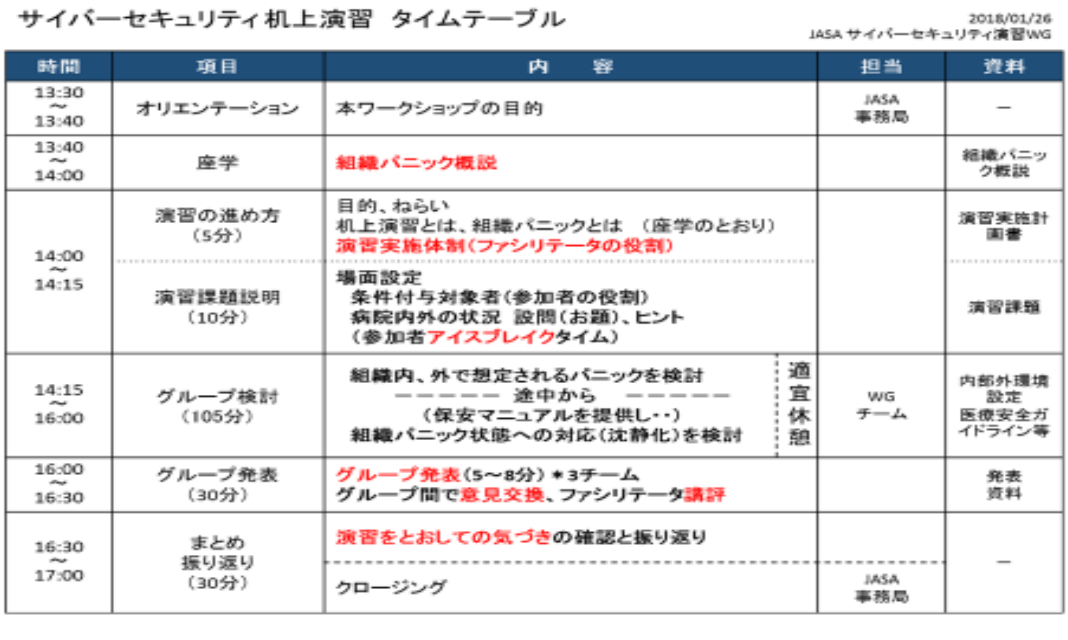
https://www.ipa.go.jp/security/fy25/reports/medi_sec/

管理医療機器（薬事法の対象）

引き金事象は、院内システム以外にも薬事法の対象となる医療機器も含まれる可能性があります。

薬事法対象の医療機器は精密機械の為、パッチ適用が出来ない例としてあげています。

１２．　演習タイムテーブル例



サイバーセキュリティ机上演習　タイムテーブル

2018/01/26
JASA サイバーセキュリティ演習WG

時間	項目	内　容	担当	資料
13:30 ～ 13:40	オリエンテーション	本ワークショップの目的	JASA 事務局	―
13:40 ～ 14:00	座学	組織パニック概説		組織パニック概説
14:00 ～ 14:15	演習の進め方 （5分）	目的、ねらい 机上演習とは、組織パニックとは　（座学のとおり） 演習実施体制（ファシリテータの役割）		演習実施計画書
	演習課題説明 （10分）	場面設定 条件付与対象者（参加者の役割） 病院内外の状況　設問（お題）、ヒント （参加者アイスブレイクタイム）		演習課題
14:15 ～ 16:00	グループ検討 （105分）	組織内、外で想定されるパニックを検討 ――――― 途中から ――――― （保安マニュアルを提供し・・） 組織パニック状態への対応（沈静化）を検討 適宜休憩	WG チーム	内部外環境設定 医療安全ガイドライン等
16:00 ～ 16:30	グループ発表 （30分）	グループ発表（5～8分）＊3チーム グループ間で意見交換、ファシリテータ講評		発表資料
16:30 ～ 17:00	まとめ 振り返り （30分）	演習をとおしての気づきの確認と振り返り		―
		クロージング	JASA 事務局	

34

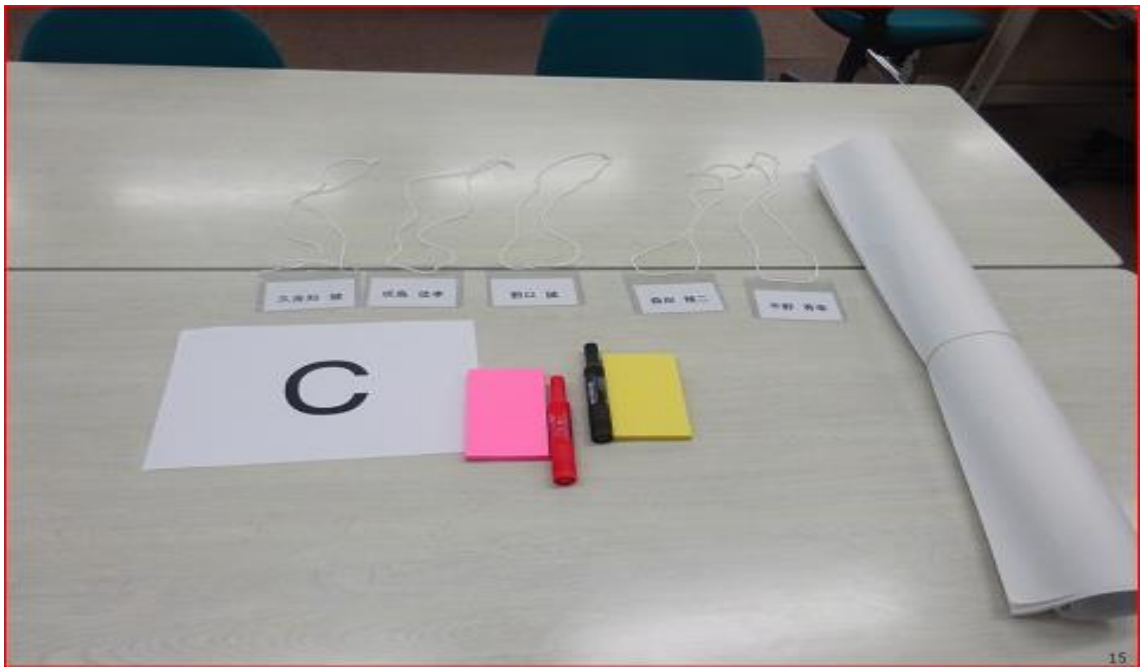
演習タイムテーブルの考え方

組織パニックを想定した演習の特性上、また参加者のスケジュールを鑑み、半日くらいの時間割が妥当と考えています。

構成要素

1　オリエンテーション
2　メインテーマの座学
3　グループ検討（休憩含み２部構成　状況を一変させる突発イベント数種含む）
4　発表
5　まとめ振り返り

１３． 演習準備（準備備品）

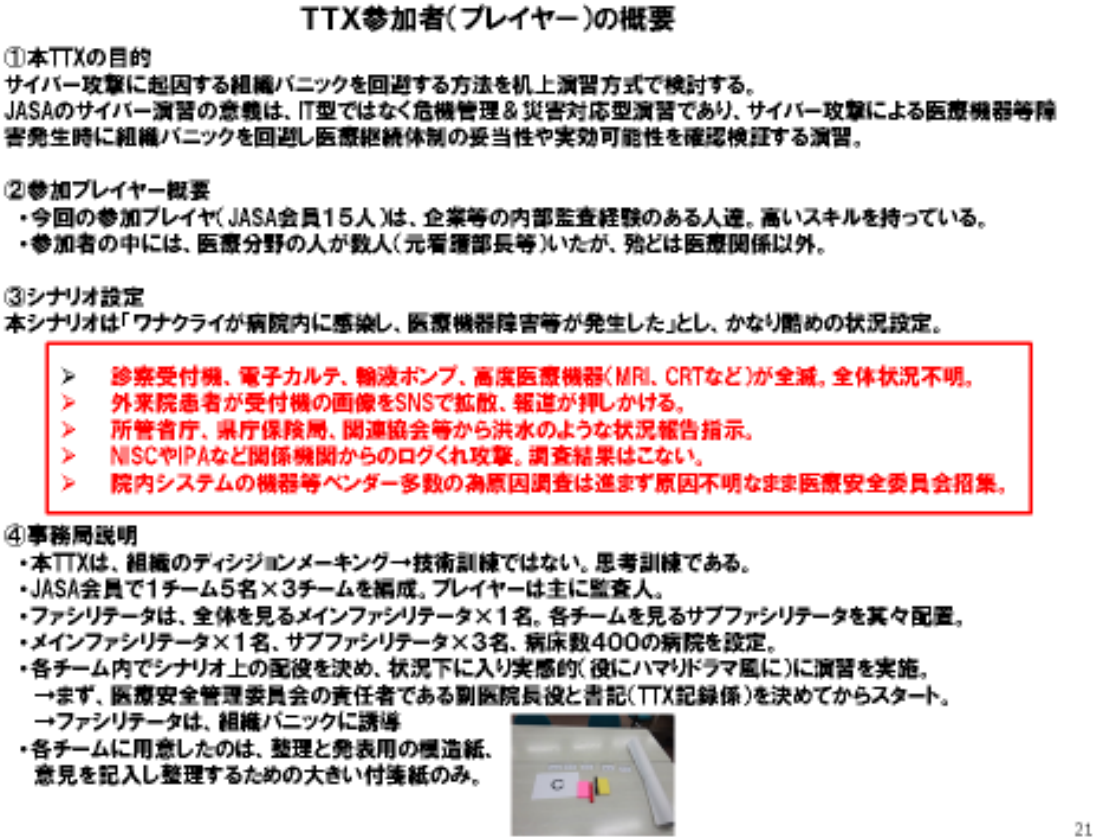


情報整理及び発表用に用意します。別途書記担当者用に記載シートも用意されています。

１４． 演習環境（配置）

１グループ各５名で３グループにしています。各グループに専用のファシリテータが付きます。

１５．　TTX 参加プレイヤの概要



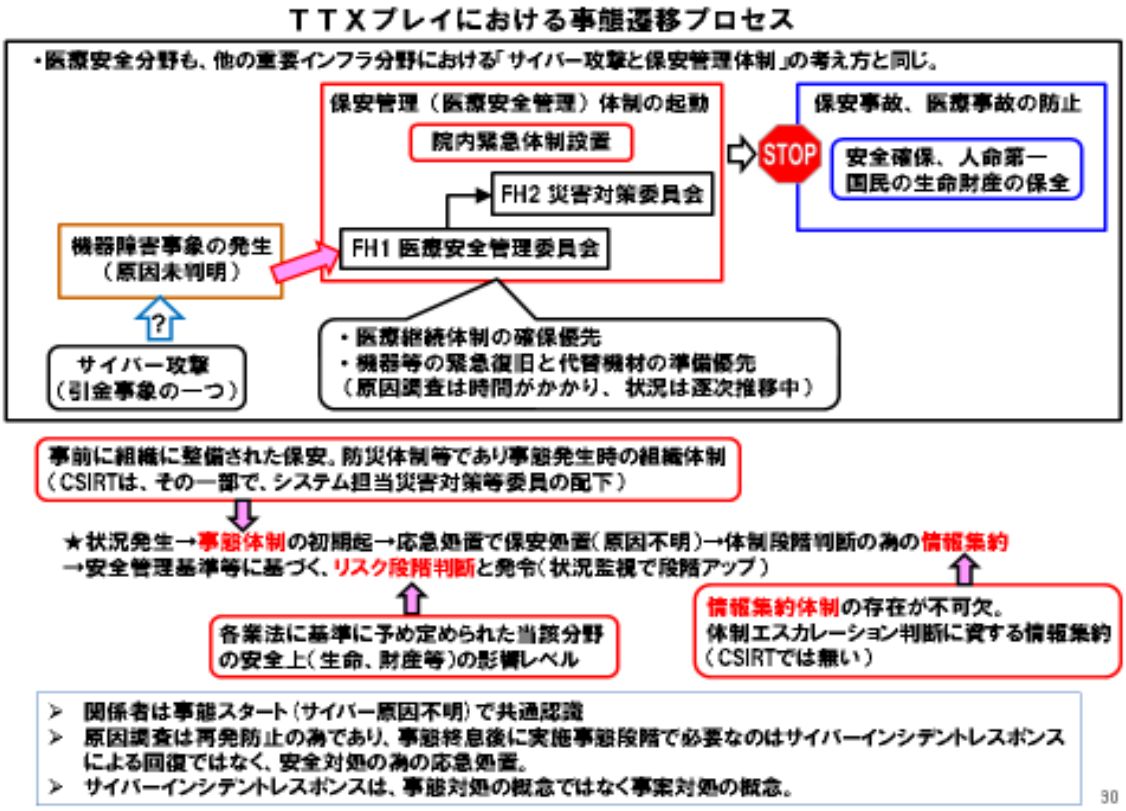
TTX の進行役（ファシリエータ）を経験している方なら、演習が狙い通りに進まず議論が発散し、もしくは演習の序盤から議論が停滞してしまう危険性を知っているかもしれません。

本シナリオの場合、医療関係者にはシナリオと実際の医療現場実態との剥離部分を指摘され、医療関係者以外には事前にシナリオで内部環境、外部環境情報を提供されているもののなぜ自分達が専門外の病院関係者を演じなければいけないのか不満を抱かれる事を懸念しました。

そこで開催案内、組織パニックの座学、メインファシリエータによる演習の進め方の説明において本演習が技術訓練ではなく、課題解決のプロセスをシュミレーションする思考訓練であることを説明しました。

しかし、本演習講座に参加する受講者は高度なスキルと高い意識を持つその道の一流スペシャリストであった為、上記の懸念は杞憂に終わり誰もが真剣にプレイヤを演じきって頂きました。

１６．　TTX プレイにおける事態遷移プロセス



TTX プレイにおける事態遷移プロセスのポイント

引き金事象であるサイバー攻撃に対して、医療システムとネットワークに繋がった医療機器の大半が使用不能、院内や院外からは問合せが相次ぎ、入院患者や、来院患者は状況を SNS に流してマスコミを中心にさらに外圧を呼び込みます。インシデントは発見時の事象であって原因の特定も、いつから侵害が発生しているかも調査段階の状態です。医療システムの回復や機器の交換は対応ベンダーに任せることしか出来ませんが交換以外復旧の見込みは立ちません。本シナリオは暗中模索状態の中で安全管理委員会を舞台に繰り広げられます。

ファシリテータ側の狙いとして院内対応、院外対応、連携する医療関係部門に対する今後の対応方針が決まった後は速やかに災害対策委員会（タスクフォース）に移行してダメージコントロールを意識しつつ、本来のミッションの陣頭指揮を副委員長に推進させることです。今回のシナリオではここまでとなっています。（グループによっては細かな演出の違いがあります。） 医療分野に限らず、リスクマネジメントは経営維持と品質の確保の狭間で厳しい経営判断を求められます。

正しい答えがなく、ケースによっては原因調査を優先することが結果として速やかな業務復旧につながることもあります。しかし熟考に欠けた性急な判断により大きな二次災害を引き起こす可能性について経営層は充分理解した上で決断をすべきです。

また、安全管理規定や緊急保安時のオペレーション体制によって事態を鎮静化するものの、更なるアクシデントを追加することでより実践的な演習になります。

１７．　TTX 参加者（プレイヤー）の意見等

TTX参加者（プレイヤー）の意見等

演習でのプレイヤ判断結果 ⇒ 本来のTTXでは、この結果を「計画等」に反映する→PDCAの“P”に該当

●医療安全管理体制
- 副委員長は直ちに「医療安全管理委員会」を招集。
- 医療安全基準（BCP）から「人命第一」優先に移行し、直ちに「医療安全管理及び災害対処体制」に移行。
- 人命優先の方針を決定。命には代えられない。当院の医療は継続する。

●医療体制
- 地域医療連携体制に基づき、他病院での受け入れも検討
- 外来患者は、他提携病院で受け入れ調整（受付機障害で診療受付が混乱）
- 外来診療でも症状の重い患者は受け入れる。
- 院内患者は、当病院で対応する。
- 入院患者の処置継続を最優先。脳疾患等患者の容体急変時は連携病院に緊急搬送。
- インフル等感染リスクを減らすための患者家族の制限を行う。

●勤務体制等
- 夜勤体制を出勤させ増強体制に移行。（機器トラブルを人でカバー）
- SNSや報道情報に踊らされることを避ける為、院内情報の保全管理も徹底。
- ナースへの指示ペーパなどは患者の目に触れさせない。

●医療機器等対処
- 高度医療機器の復旧を優先。連携病院から機材を借りる等の手配を直ちに実施。
- オフラインで使えるシステムは、ネットワークから応急的に切り離した。
- システム復旧と原因調査は、事態が落ち着いた後となる。
- 電子カルテは応急バックアップと追加ヒアで使用し、復旧は７２時間以内とした。

●外部対応
- 外部（報道、NISC、JPCERT、IPA等）から色々確認がくるが、厚生労働省への対応を優先。
- 騒いでいる報道対応は、広報室が担当。
- 外来患者等によるSNS発信（報道が見てる）には、病院のツイッターから情報発信。

演習参加者（プレイヤ）の感想意見

●全般
- 各人、役を演じ切っていた。ドラマを見てるような感じ。
- 当初、サイバー訓練という事でよくある技術訓練かと思ったが、これは「危機管理訓練」だと気がついた。多くの気づきを得られ、大変良かった！
- サイバー演習と言いながら「マルウエア解析」「連絡網の確認」が多い中、「状況把握」「情報共有」「判断」の演習であることに気付いた。
- 普段は会社で指示する立場であるが、今回は指示される側。不要不急の指示はしない事が重要と体験した。

●医療安全管理
- 病院とは、元々危機管理体制を敷いている組織体。常に増強人員（シフト）を確保している。
- 本TTXは、ゴール（対処目標マイルストンなど）が見えやすかった。
- 各プレイヤー及びサブファシリテータは迫真の演技だった（実際の状況に近い中での検討議論が出来た）
- 普段の病院は人的リソースのMAXは使っていない。いつでもシフト勤務リソースを投入可能にしてある。
- 大抵の事は、アナログで回る体制を取っている（手動の輸液ポンプの配備等）。
- 阪神大震災の教訓も生かしている（報告書もあり）。

●気付き点
- 当初、手順に議論が行く傾向があった。
- 前半は議論白熱で内容的に深い議論を活発に実施。その結果、副医院長は追い詰められた。
- 医療安全管理委員会の責任者として、腹をくくる必要があった。
- 上がバタバタしない事が大事。でないと話（技論）が収束しない。
- 最初システムの調査に指向しかかったが、「人命優先」により「医療安全管理及び災害対処体制」に移行。
- 「システムより人命優先」が勉強になった。（技術解析視点と医療安全管理体制視点）

１８．　病院においける医療安全管理指針と医療安全管理規定の重要性

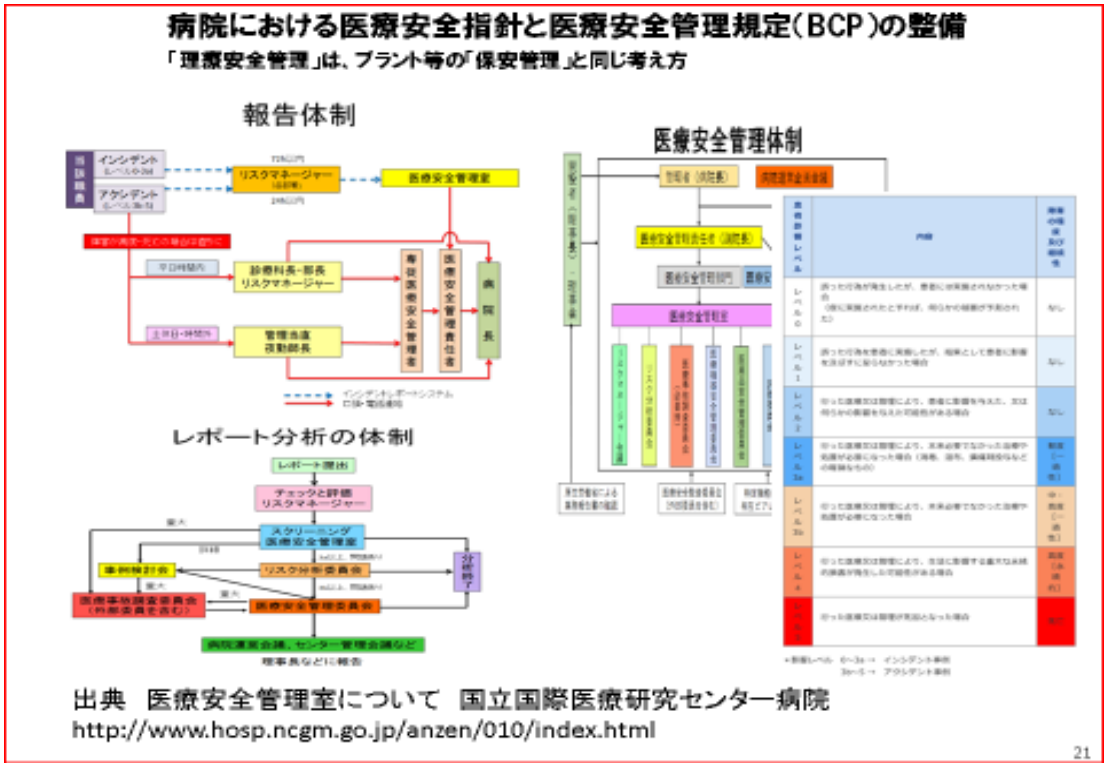
演習参加者（プレイヤ）の感想意見

●システム部門

- **当初、情シスにトラブル状況を確認したが解らない（ファシリテータから調査中との状況付与）。**
- **事象発生から午前中は、緊急リカバリとバックアップデータの応急復旧に当たった。**
- **その後、やっと調査に入れたが、原因等は依然不明なまま、「医療安全管理及び災害対処体制」に入った。**
- **電子カルテ、高度医療機器、輸液ポンプなど、全てのシステムの把握が必要だが、各システムはバラバラのベンダーであり、情報（状況）が集まりにくい。→システム群把握に関する体制を要検討**
- **NISCにログを提供したが、調査結果は直ちには来ない。かつ院内状況はどんどん推移。**

●引金事象としてのサイバー攻撃を認識

- **サイバー攻撃は機器等障害原因の一つ。病院の「医療安全管理及び災害対処体制」として行うべきことは変わらない。他の障害等原因（地震、停電等）と同じ扱い。**
- **BCPは自然災害を想定したものであり、サイバー攻撃時のBCP及び訓練が必要と感じた。**
- **但し、サイバー攻撃による機器等影響は、引き金事象であり機器等影響発生後の対応は「医療安全管理及び災害対処体制」に従って行う事になる。**



インシデント対応目線から本来の保安管理目線（アクシデント対応）への切り替えの契機となる医療安全指針と医療安全管理規定（BCP）の整備が重要です。

１９．　TTX による組織パニックの検証結果

本TTXによる組織パニックの検証結果

★医療安全管理体制

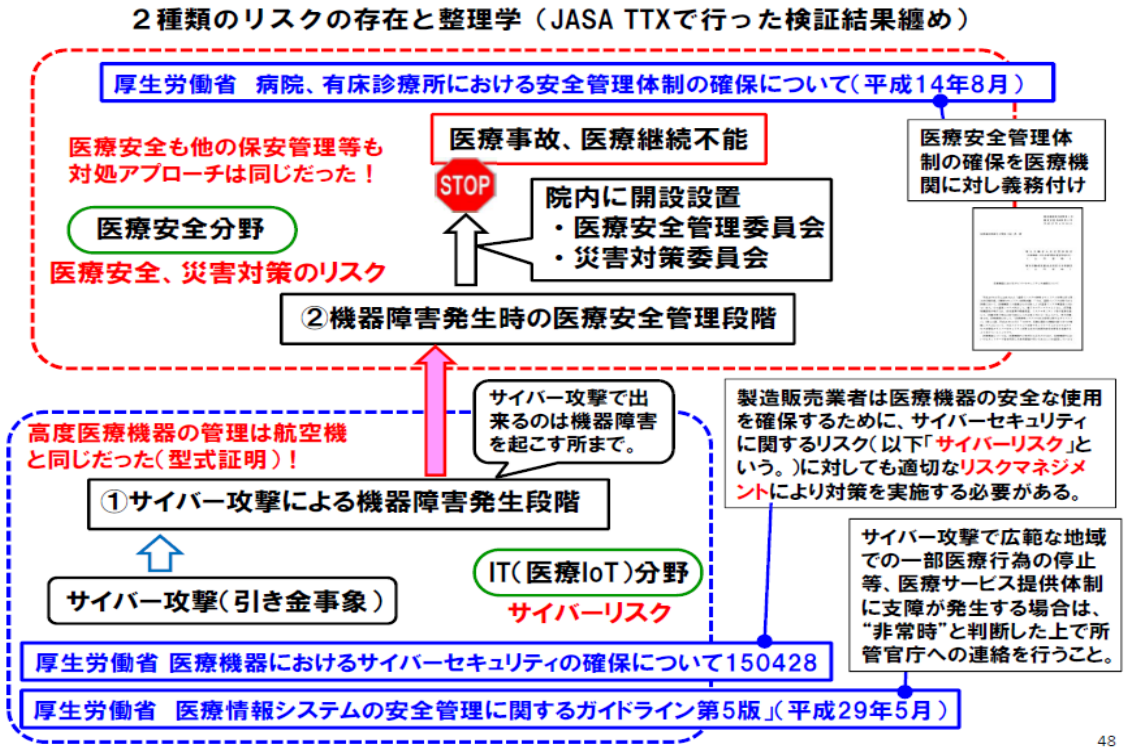
- **病院自身は災害対応を前提とした危機管理型組織であるため、医療安全基準等に基づく安全体制が整備されてる。**
- **このため、病院そのものは組織パニックにはならなかったが報道や官庁等の外部組織が組織パニックに至る。**
- **医療安全管理は、プラント等他の保安管理と同様の安全に関するアプローチを取っている。**
- **サイバー攻撃で起こせるのは医療機器の障害のみであり、機器障害発生以降は医療安全管理基準に基ずく対応を行う。**
- **このため、サイバー攻撃のみで、患者が死ぬようなことは無い。**
- **他国の医療安全管理体制は日本程整備されていない可能性がある。**
- **他国事例を参考にする場合は、医療安全管理体制部分を確認する必要がある。**

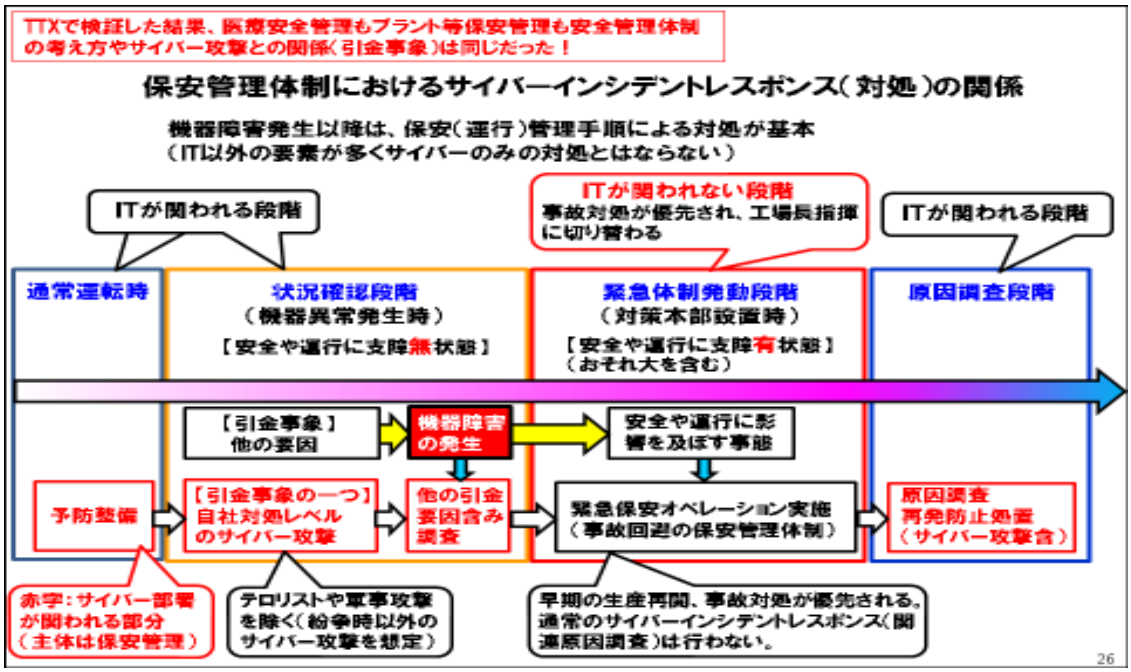
★組織パニックが起きなかった要因

- **「人命優先」という統一した目的を職員全員が共有で来ている。**
- **医療安全は「ダメージコントロール」の概念を持っている。**
- **サイバー攻撃含め「引金事象」の概念を持っている。対応は従来から整備してる医療安全管理体制で対応可。**
- **医療安全管理委員会が「防災指揮所」として機能している。**

　演習参加者はほぼ医療関係者ではありませんが、組織運営の基本を熟知していれば良識の範囲で多くの洗い出すべき課題と対応方針の策定を実施することが出来ます。
今回は実際の緊急医療に携わった経験豊富なプレイヤが参画していた為、患者や患者の家族の心情、医療提供側特有の事情、様々な利害関係者の人間特性まで踏まえたきめ細やかな配慮がなされています。
　もしこのシナリオを医療関係者のみで行う場合は、さらに踏み込んだ具体的な課題と対応策が洗い出されるでしょう。条件付与による突発アクシデントもより判断が難しく、即決即断を求められる課題を与えてみるといいかもしれません。一般的にこのようなシナリオでは判断を仰ぐ上司は不在か、組織パニックに飲み込まれて責任を伴う一切の判断をしない場合が通常です。さらに酷い場合は自己保身の為にさらなる二次被害が発生する引き金を経営層自ら扇動してしまう可能性があります。
　そこは上司の判断も仰げない、近視眼的な対応しか出来ない組織では踏み込めない領域になります。自分達の為すミッションが全体の中で何を担っているか理解していれば業務システムやネットワークを遮断、パッチを適用という提言が事態案件時では相手方の環境や風土、文化を考慮しない極めて安易な回答であるとわかるはずです。実際に世界を蔓延し現在も亜種の被害が増加しているランサムウェアに対して、（一部人命最優先もしくは最短で業務復旧を期待できるためにあえなく身代金を支払う医療機関があったものの）多くの医療機関は危機管理の範疇とみなしリスクアセスメントとトリアージを駆使して、ダメージコントロールによる業務継続を断行しました。医療機関の緊急事態という非日常空間は、特殊ではあるものの対応の仕方は災害時における事業継続と同様サイバー攻撃は引き金事象に過ぎず、気を付けるべきは組織内外に発生する扇動的な流言飛語に振り回されないことと言えます。

２０．　演習のまとめ　２種類のリスクの存在と整理学





今回の演習では、サイバー攻撃を引き金として 2 種類のリスクをまたがり、その脅威に対する対処が業種業態を問わないことを改めて検証することが出来たことです。また興味深いことにアクシデントが沈静してからは原因究明や再発防止策の策定で IT が問われる段階に戻ることから視点の切り替えは必要ですが改めて IT であっても全体を俯瞰する姿勢が重要であることも再確認できました。

おわりに

１．演習の反省点

今回は TTX の基本的な考え方を理解するためにリスクアセスメントによるリスクの分類（【回避】【移転】【軽減】【保有】）や CERT シナリオで見受けられる D-OODA（【Design】【Observe】【Orient】【Decide】【Act】）といった米軍式のオペレーション・デザインまではあえて演習目標に反映しませんでした。インシデント対応シナリオを予想していた参加者は大変恐縮ですがご容赦ください。

条件付与のタイムラインの明記が不十分でプレイヤの方々に戸惑わせてしまうことがありました。議論の内容にも明らかにかかわる必須の情報の為今後の反省点にさせて頂きます。

想定以上に組織パニック時の問題の洗い出しが噴出し、見事に緊迫した状況を再現していただいたものの洗い出しが多すぎてエンドレスになりかけたグループがありました。左記のような場合は長くても 10 分くらいの時間を目途に振り返りやまとめに移行するなど進行を見直します。

事前の告知が行きわたらず、大変ありがたいことに事前に模範回答までを作ってくださった参加者の資料をご紹介する時間を用意できませんでした。深くお詫びを致します。

２．新たな人材層の育成、発掘、再発見

本 WG にとっても異なる領域を横断してクライシスマネージメントする橋渡し人材にはどのような人材像、人物像がふさわしいか考えさせられる良い機会になりました。

各方面に対して造形が深いプロフェッショナルなら誰でも出来ることでしょうか。

もちろん経営者に信頼されていれば条件は問われないはずです。

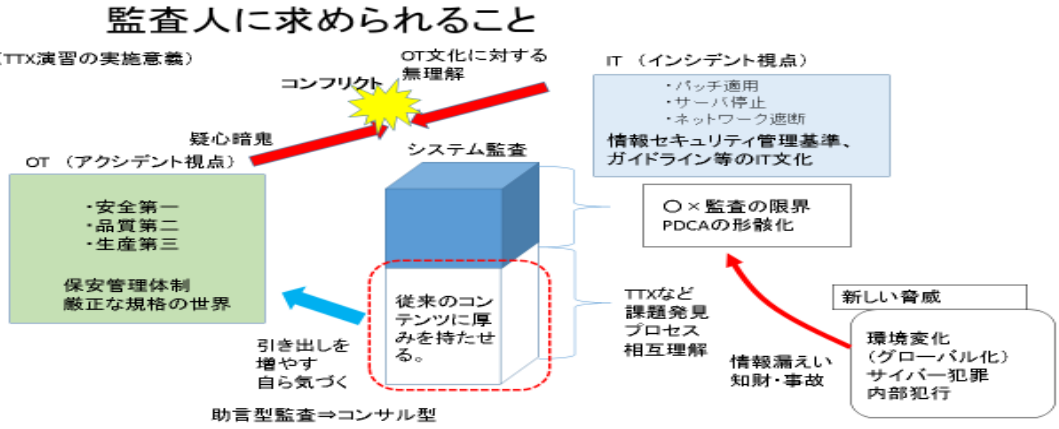
ただ、実績もない人が信頼を勝ち得るにはかなり長い信頼構築期間が必要です。

では、最初から経営者に信頼されている経営者の先輩達ではどうでしょうか。

そのような人材はもう第一線を離れている人が大半かもしれません。

多くの人に信頼された実績を持ち、多くの危機を乗り越えた貴重な経験をしてきた先輩達こそ有事において真価を発揮する人材として今後の組織には必要かもしれません。

３．今後の監査人に求められること



WG の活動を通して今後の情報セキュリティ監査人のあるべき姿、方向性が見えてきました。

活動履歴

ファシリテータ養成講座　全３回（2017 年１月～４月）

第一期　活動実績　　全９回（2017 年７月~2018 年２月）
第１回：2017 年　７月 21 日
第２回：2017 年　８月 25 日
第３回：2017 年　９月 22 日
第４回：2017 年 10 月 27 日
第５回：2017 年 11 月 24 日
第６回：2017 年 12 月 20 日
第７回：2018 年　１月 17 日
第８回：2018 年１月 26 日（JASA 会員向けサイバーセキュリティ机上演習ワークショップ開催）
第９回：2018 年２月 20 日（報告会検討）

成果物（作成者　WG メンバ全員　メインライター　小川敏治氏）
シナリオ実施計画書
医療シナリオ（本体）
・内部環境・外部環境設定資料（シナリオ用）
・医療安全指針と医療安全管理規定（シナリオ用）

活動メンバ一覧（1 月 26 日ワークショップ出席貢献者含む）

	名前	所属	チャレンジコイン取得
1	内藤　剛 （総合ファシリエーター）	NEC フィールディング株式会社	○
2	小川　敏治 （座学講師　シナリオライタ）	ｏｎｅ株式会社	○
3	菊地　宏紀 （技術・演習支援）	株式会社インフォセック	
4	野村　一彦 （技術アドバイザ）	株式会社インフォセック	
5	小西　直人 （技術・演習支援）	レプリゼント株式会社	
6	坂本　美子 （隊長補佐官兼事務総長）	株式会社日立システムズ	○
7	石崎　仁 （技術アドバイザ）	セイコーエプソン株式会社	
8	野嶽　俊一 （CIO 補佐官兼演出家）	株式会社インテック	○
9	福岡　かよ子 （総監督兼タイムキーパ）	株式会社インテック	○
10	柳澤　智 （庶務担当）	富士通株式会社	○
11	山田　夕子（私立病院に勤務する唯一のＣＡＩＳ）	社会医療法人愛仁会	
12	下村　源治 （構成作家兼技術顧問）	パーソルホールディングス	

WG 運営事務局

	名前	所属	備考
1	永宮　直史 （WG オーナー）	JASA 事務局	
2	柳澤　幸子 （WG 推進担当）	JASA 事務局	
3	安藤圭二 （WG 支援担当）	JASA 事務局	

スペシャルサンクス

協働の会総合プロデューサ　兼　組織パニックエバンジェリスト

JNSA　脅威を持続的に研究する WG より TTX 演習指導員として招いた

岡谷　貢　隊長（元戦闘機のパイロット）

出典　変化する“情報セキュリティ”の意味、防衛庁統合幕僚監部の岡谷氏が講演

https://internet.watch.impress.co.jp/cda/event/2006/10/05/13530.html

Plus Ultra(プルス　ウルトラ)

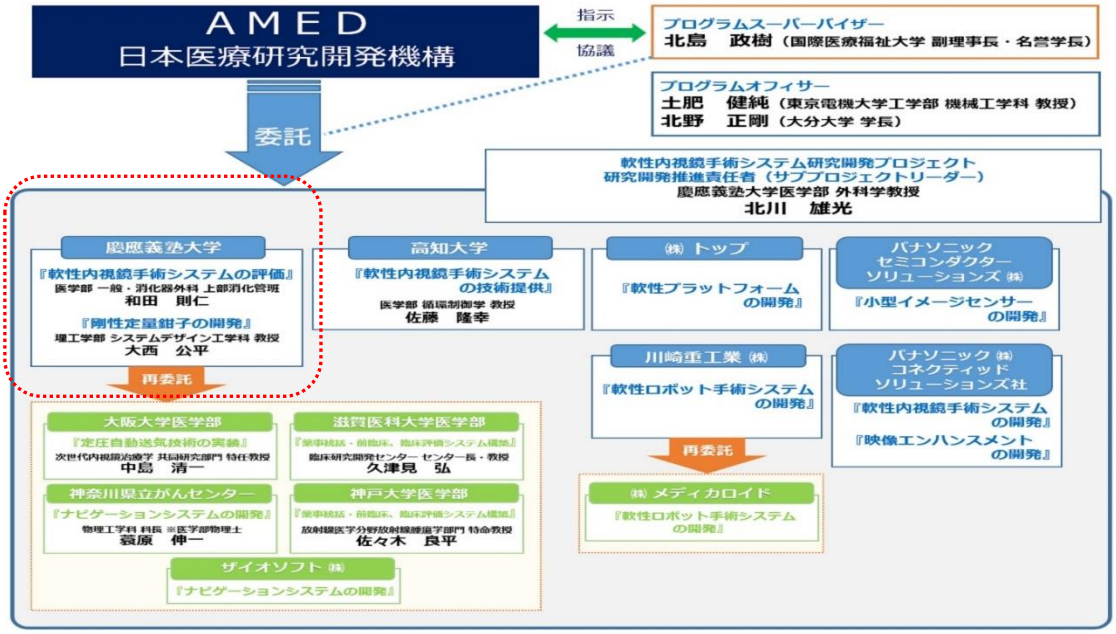
困難なミッションに組織を超えて攻略しよう　そこには絆が待っている by 亀山社中

謝辞

IDF 医療 WG　理事長　和田　則仁　先生（ＦＥＳＳ開発プロジェクト）
慶應義塾大学医学部外科学（医学部　一般・消化器外科　上部消化管班　専任講師）

医療シナリオの構成を考えるにあたり、病院の危機管理能力に関する取り組みや最先端の医療機器の現状に関してご教授してくださいました。手術ロボットによる遠隔治療の国内の開拓者であり、医療行為の可視化、医療機関におけるデジタル・フォレンジックの可能性を研究しています。

出典　http://www.surgery-med-keio.jp/original16.html#anc01



出典　医療分野におけるデジタル・フォレンジックの可能性

謝辞

本 WG の為に講師として参加してくださったセキュリティ及び有識者としてご助言くださった方々

内閣官房　情報通信技術（ＩＴ）総合戦略室　政府 CIO 補佐官　根本　直樹　様

株式会社　日立システムズ　技師長　本川　祐治　様

一般社団法人　JPCERT コーディネーションセンター　常務理事　有村　浩一　様

一般社団法人　JPCERT コーディネーションセンター　早期警戒グループ　佐々木　勇人　様

EY アドバイザリー・アンド・コンサルティング株式会社　シニアマネージャ　森島　直人　様

カスペルスキー　情報セキュリティラボ　セキュリティリサーチャー　石丸　傑　様

カスペルスキー　情報セキュリティラボ　セキュリティアナリスト　大沼　千亜希　様

国立情報学研究所アーキテクチャ科学研究系教授　高倉弘喜　様

参考文献

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（著）

『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語る戦略論。

折木 良一（おりき・りょういち）元自衛隊第３代統合幕僚長

組織パニック時の指揮官のあり方を講義する折木　元第３代統合幕僚長

事故から学ぶ多重防護層の設計

○伊藤 利昭（元名工大）村外 敬助（三菱化学㈱）安部 貴巳弘（㈱エステック21）

https://www.jstage.jst.go.jp/article/jacc/57/0/57_903/_pdf

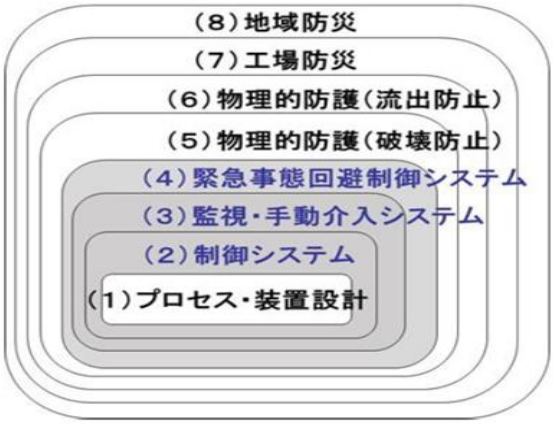


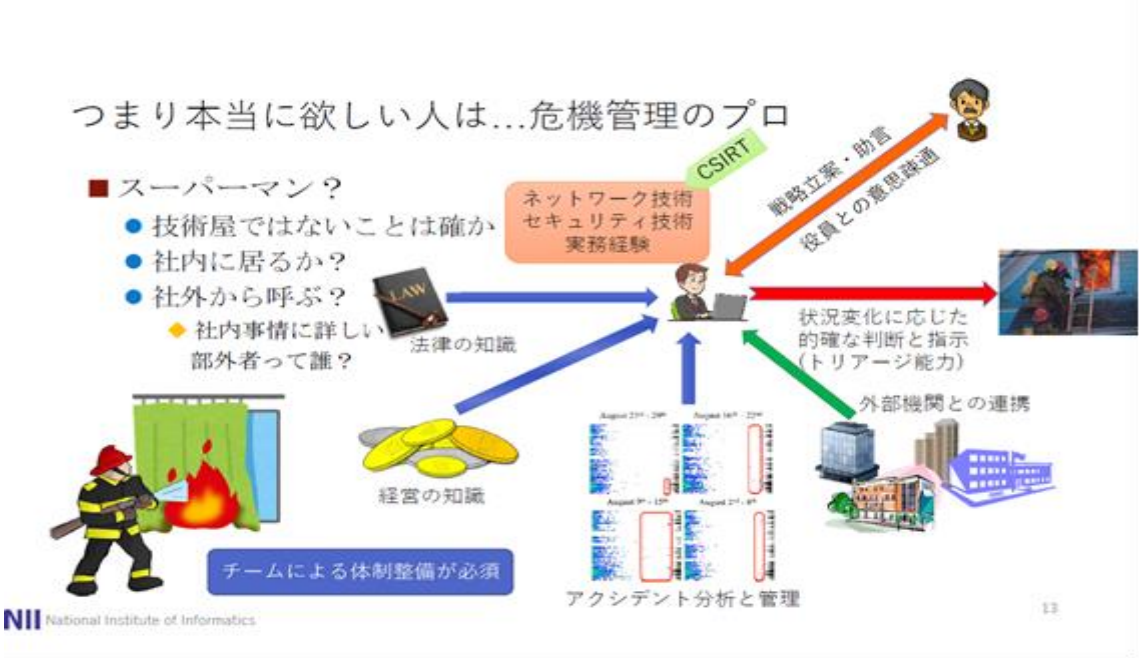
図１ AIChE/CCPCによる多重独立防護層

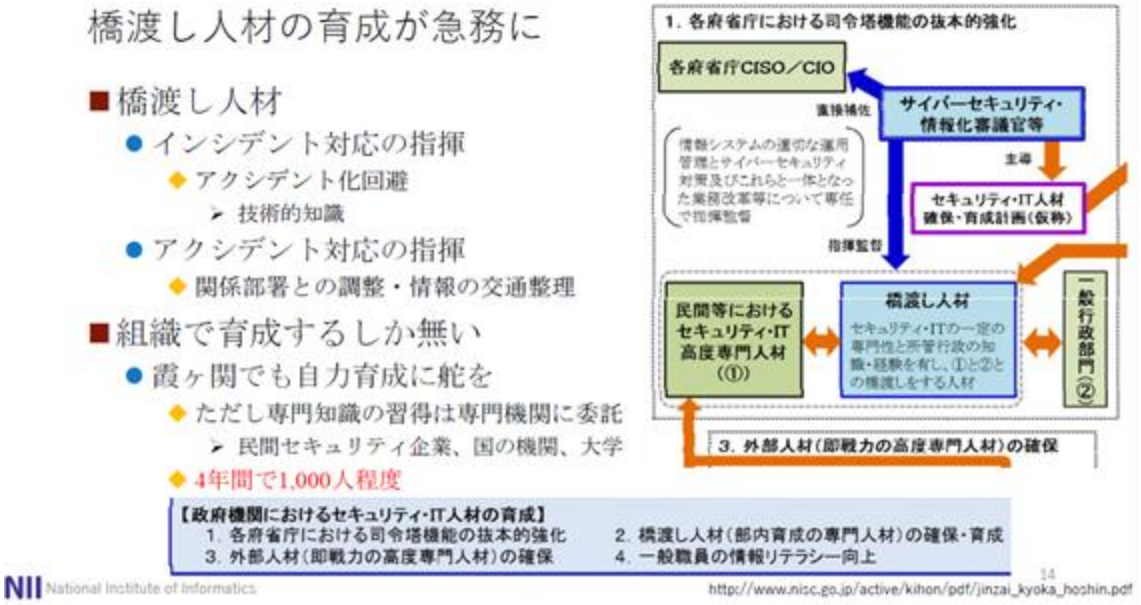
「日本型組織」はなぜサイバー攻撃に弱いのか

PwC サイバーサービス合同会社 最高技術顧問 名和利男

https://www.pwc.com/jp/ja/services/cyber-security/seminar/vol1.html

第二期（セカンドシーズン）に向けて方向性の再確認





出典　国立情報学研究所　アーキテクチャ科学研究系教授　高倉弘喜著

危機管理時における情報管理　～エリートパニックを引き起こさないために～

www.rman.jp/meetings2017/doc/I-1_1.pdf

演習の評価測定に関するヒント

出典　東京海上日動リスクコンサルティング株式会社
危機管理グループセイフティコンサルタント　北村　和彦　氏著

本番で役立つ危機管理演習/訓練体系

www.tokiorisk.co.jp/risk_info/up_file/200412292.pdf

MSEL を使った演習指導計画書の作成要領の骨子

www.tokiorisk.co.jp/risk_info/up_file/200512281.pdf

After　Action　Review という評価法

www.tokiorisk.co.jp/risk_info/up_file/200412294.pdf

Presentedby　JASA