サイバーセキュリティ・インシデント対応机上演習

TTX; Table Top eXercise

小出　洋

九州大学
情報基盤研究開発センター

小出　洋（こいで　ひろし）

JavaOne2009 SunSPOT BOFにて

Twitter　@hirosk
Facebook　Hiroshi Koide

経歴

日本原子力研究所計算科学技術推進センター
↓
九州工業大学工学部（戸畑）
↓
九州工業大学情報工学部（飯塚）
↓
九州大学　情報基盤研究開発センター　副センター長
サイバーセキュリティセンター（2017.4～）
システム情報科学府（2017.6～）

社会貢献

- ☆ **SECCON実行委員**
- ☆ **セキュリティ・キャンプ in 福岡**
- ☆ **福岡県警サイバー犯罪テクニカルアドバイザ**

得意分野

- ☆ **プログラミング**
- ☆ **サイバーセキュリティ**

（Moving Target Defense, 脅威トレース…）

Awards

- ☆ **IPA スーパークリエータ**
- ☆ **JavaOne 2005 Duke’s Choice Award**
- ☆ **Sun Microsystems Center of Excellence**

One of my hobbies (Making something)

夏向けの真空管アンプ

★6 ◉3598

74HCU04パラレルアンプ

★5 ◉4981

Arduino Mega でポケコン

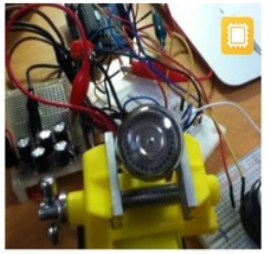
★5 ◉3343

Raspberry Pi ロボットカー（カメラ付）

★1 ◉2403

RasPi+USB-DAC ミュージックサーバ...

★1 ◉2559



Dekatron 遊び

★1 ◉1752

駄球 5AT8 シングルアンプの試作

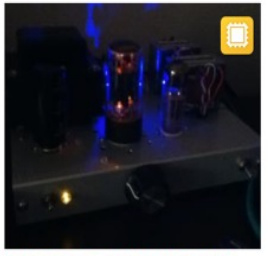
★2 ◉2184

6MJ8 シングルアンプ

★2 ◉1913

バーボンな音がするスピーカをつくってみた

★2 ◉2144



USB DAC を積んだ7号機

★1 ◉1723

真空管ドライブ 6A6 B級PPアンプ

★1 ◉2441

6AT8 シングルアンプ改

★0 ◉2353

【安価】5AT8 シングルアンプ

★2 ◉1937

ユーハイムな音がする4号機

★2 ◉1142

SunSPOT インベーダ

★2 ◉1303

6AT8シングルアンプ（ニッケル水素充電池バイ...

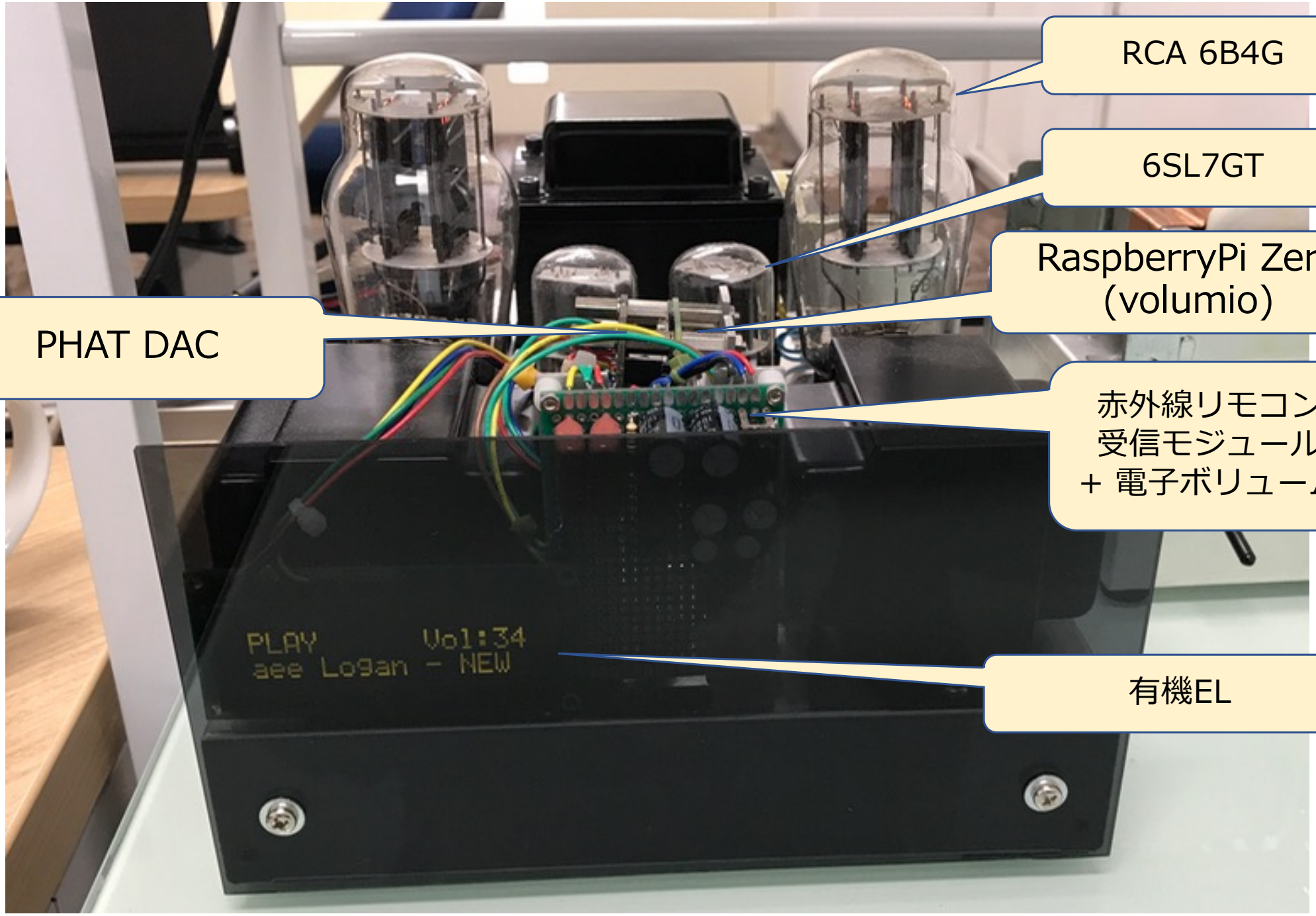
★0 ◉2520

直熱管☆33シングルアンプ☆スタイリッシュ！

★0 ◉1826

Sun SPOT ガイガーカウンター

★0 ◉1118


RCA 6B4G
6SL7GT
RaspberryPi Zero
(volumio)
PHAT DAC
赤外線リモコン
受信モジュール
+ 電子ボリューム
PLAY Vol:34
aee Logan - NEW
有機EL

これまでの話題

第0弾

究極のサイバーセキュリティ対策

～人材育成：九州大学での社会人サイバーセキュリティ教育の取り組みと地域・コミュニティの連携～

2021/2/3 14:15～14:45

地域セキュニティを盛り上げていこう！

第1弾

地域セキュニティにおける産官学の連携について考える

2021/9/28 15:10～15:40

産官学のそれぞれのステークフォルダの連携が肝要

第2弾

ビジネスに必要なサイバーセキュリティの要素

2021/10/28 14:20～14:50

サイバーセキュリティが持つ科学的特徴の性質からビジネスに必要なサイバーセキュリティの要素について考える

第3弾

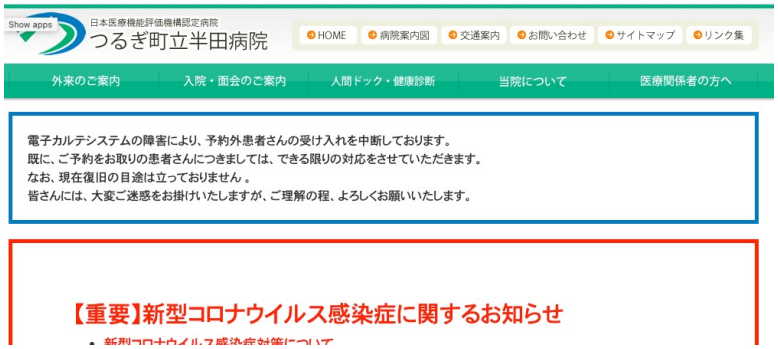
変動標的防御の紹介

2021/11/10　14:10～14:40

小出が研究しているMTD（Moving Target Defense）について紹介

医療現場で電子カルテシステムにランサム被害の現状

奈良宇陀市立病院 2018.10



徳島つるぎ町立半田病院　2021.10

米国アラバマ州スプリングヒル・メディカル・センター　2019.7

組織におけるミッションとは

例えば．．．

- 大学のミッション
  - 教育
  - 研究
  - 医療（医学部のある大学）
- 病院のミッション
  - 役割に応じた医療を提供し続ける

このミッションを継続することが組織の使命！

病院におけるミッションは人命に関わる

- 法にもとづき，具体的かつ実効性のある体制を整備
- 事業継続！
- 日常・平時と同じパフォーマンスで医療を提供するのがベスト
- さまざまな事情で病院がいつもの状態でいられないのは問題（ex. コロナ禍）

TTX（Table Top eXecerise）机上演習

TTXの目的

- 事業継続に関連する「体制の検証」
  - BCPを作成しただけでは不十分．つまりそれに伴う体制も検証しなければ不十分
  - 常に想定外のことがおきるかもしれない
  - 予期しないものは準備できない
  - 事前に体験演習　→　問題点・課題を洗い出し　→　BCP作成に資する
  - 実際にやってみることで見えてくることがある（気づき）
  - 120パーセントの準備
  - 検証を行うことでBCPの精度を向上することが可能（欠落事項など）

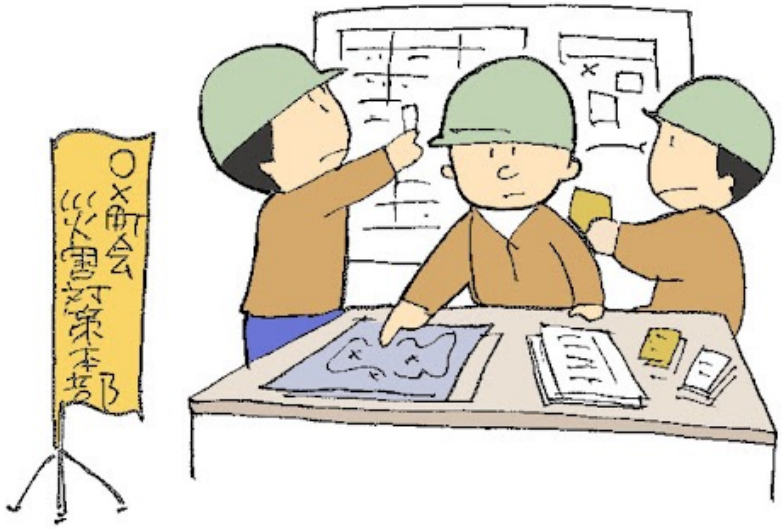
TTX（Table Top eXecerise）机上演习

- TTXとは…
  - 実際に近い Role Play 形式で具体的かつ実際的なシナリオを用いた演習
  - （少なくてもBCP体験型机上演習は）机上では行われていない
    - 机上で行われるから机上演習ではない
    - 「オリエンテーション」というイメージが近い
  - 対象となる問題を深く理解可能とする
  - 事前に体験することにより対処の余裕が生まれる

BCP体験型机上演習

- 「BCP型TTX」とは，**サイバー攻撃が引き金事象**となり，「組織対応事態」に至った場合の「対策本部活動」を通じ，「サイバー攻撃事案とBCP（事業継続）」の関係を模擬体験するTTXを指す
- サイバー攻撃対応とBCP対応の問題を一体にしたTTXは他に事例は無い

↔ 問題検証型TTX，インシデントレスポンス型TTX

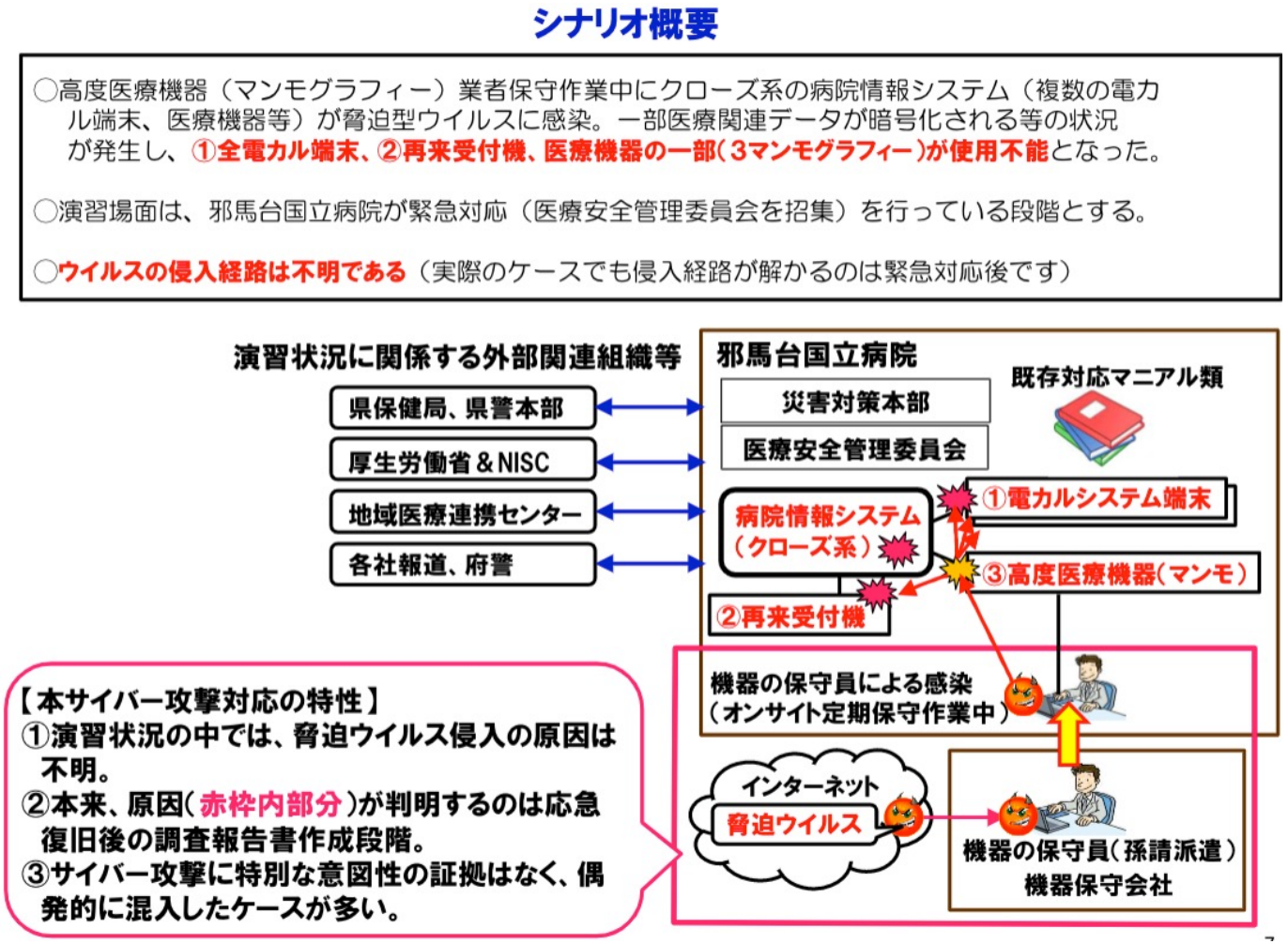


BCP体験型机上演習

- 九州大学 SECKUN/ProSec-IT におけるBCP体験型TTXでは．．．

  - ランサムウェアによるインシデント（引き金事象）が題材

    - 対策本部でのITセキュリティ部署（CSIRT等も含む）の役割は何か
    - 病院独自の要素や医療安全の考え方
    - 身代金の支払いに対応するか
    - 優先すべきことは何か（原因究明？組織のミッションは何か）
    - 演習状況に関連する外部関連組織への対応



BCP体験型机上演習

- 九州大学 SECKUN/ProSec-IT におけるBCP体験型TTXでは．．．

  - 実際的なシナリオを使った机上演習
    - 病院関係者からのヒアリングに基づく
    - Roleplay による体験型BCP演習

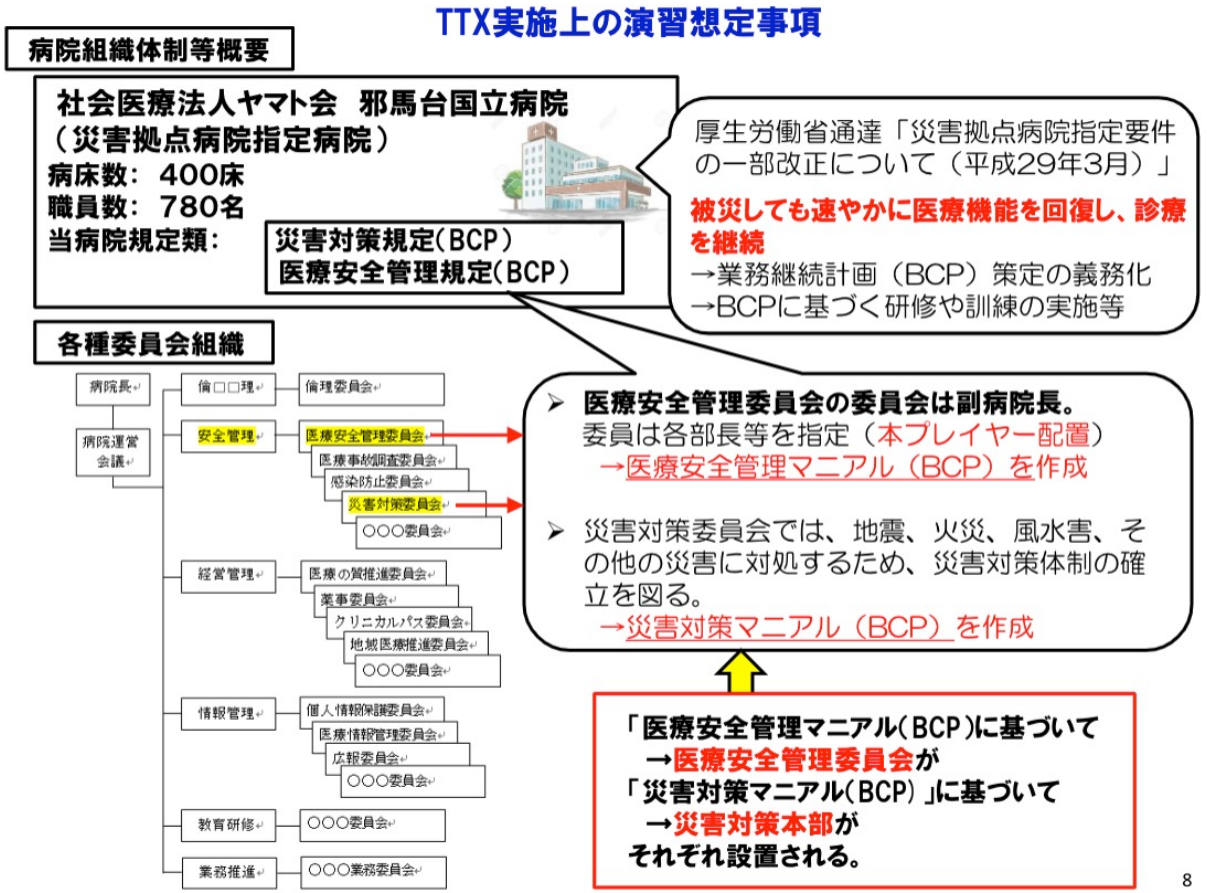
    → マスコミ対策やトラブル患者対応も含まれる

    → 体験してみることにより見えてくる「気づき」がある

    → 参加者どうしの議論を行い，問題を整理するフェーズもある

    → 実際のインシデント対策と事業継続に資する

  - 地域セキュニティとの連携でまっさきに取り上げられた「演習」



BCP体験型机上演習

演習で題材にしているランサムウェアとは？

- 感染するとファイルを暗号化し使用不能とする
- 犯人は、暗号化ファイルを復号し使用可能状態に戻すための金銭を要求（脅迫）してくる
- ばらまき型マルウェアのひとつ（ばらまき型だが病院をターゲットにすることも多い）

実際に病院で展開されているTTX事例

- 亀田メディカルセンターの事例

Yahoo!ニュース

亀田メディカルセンターがシステム障害に備え訓練　鴨川（千葉県）（房日新聞） - Yahoo!ニュース

鴨川市の亀田メディカルセンターはこのほど、電子カルテを中心としたデジタルシステムが突然使用できなくなったことを想定した、システムダウン訓練を実施した。対策本部の立ち上げなどの実働と机上訓練で、対処を (265 kB)

https://news.yahoo.co.jp/articles/2fe475396593ceeea3b0c6841131af285b1604cc?fbclid=IwAR0vxPylBKvhrd2pCTApb1OzmjpPAMXch8CBJGHgvzkcHsap6b83hKY1lC8

九大におけるTTX（2019年の様子）

岡谷貢隊長

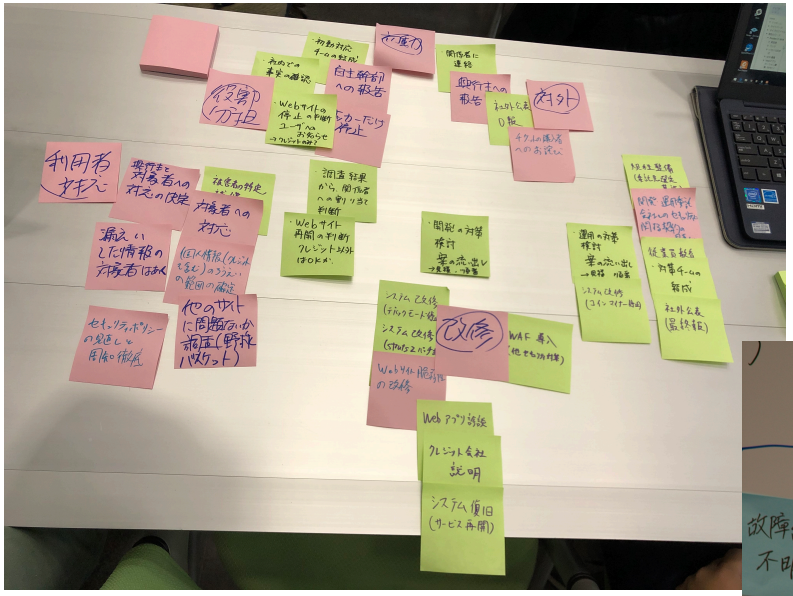
TTX・・・Table Top eXercise（机上演習）

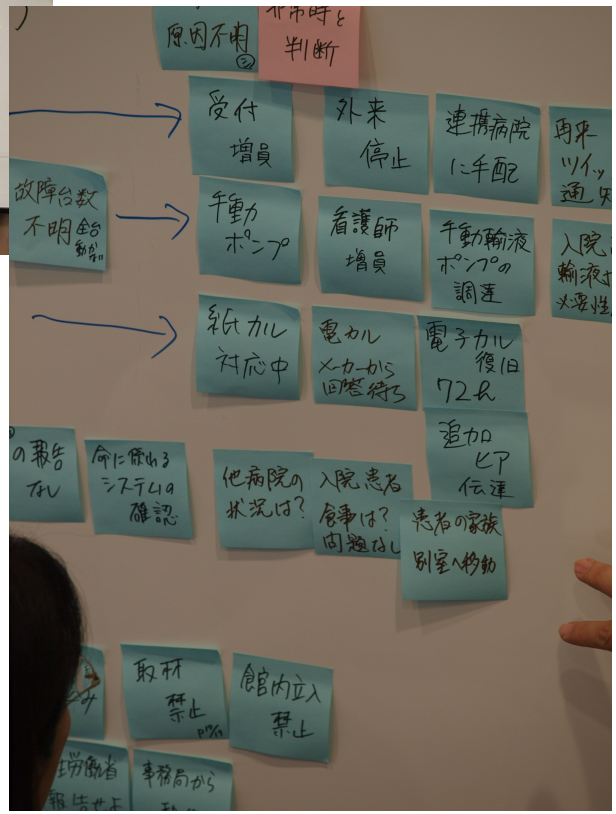
詰める・詰められる・エクササイズ

→計画やルールに不備はないか、実戦形式でチェック

※受講生の最終成果報告会のスライドから抜粋

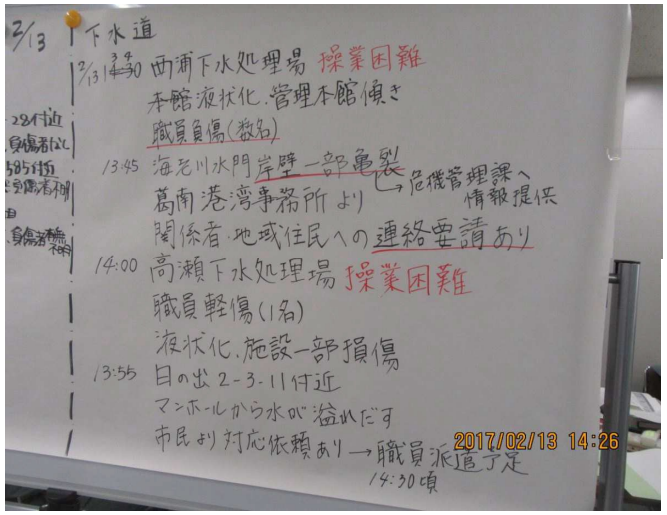
九大におけるTTX（2019年の様子）

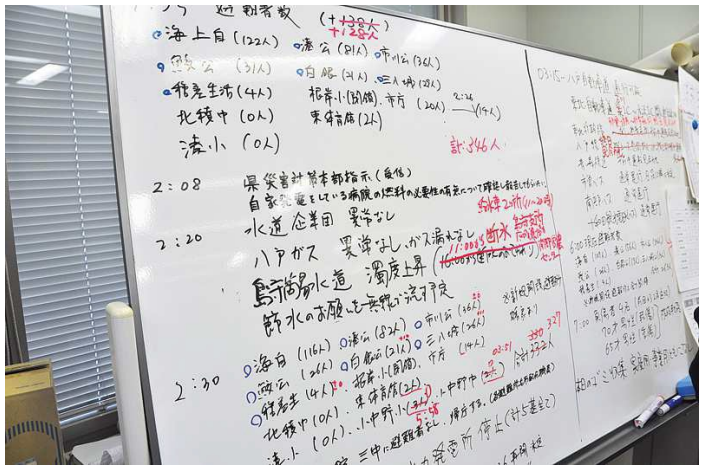


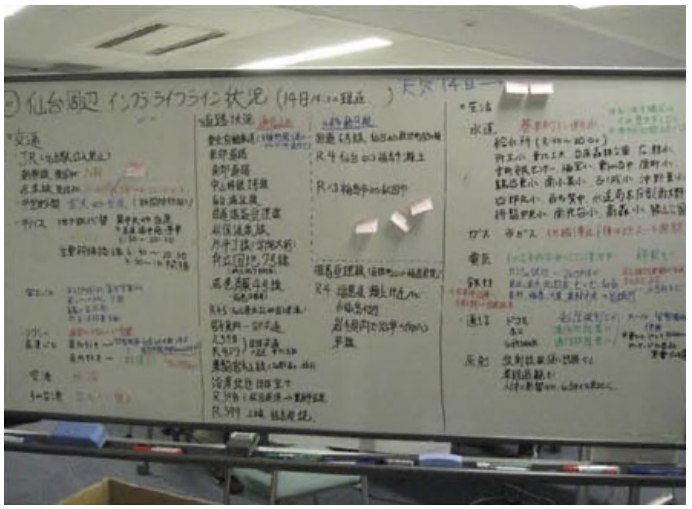


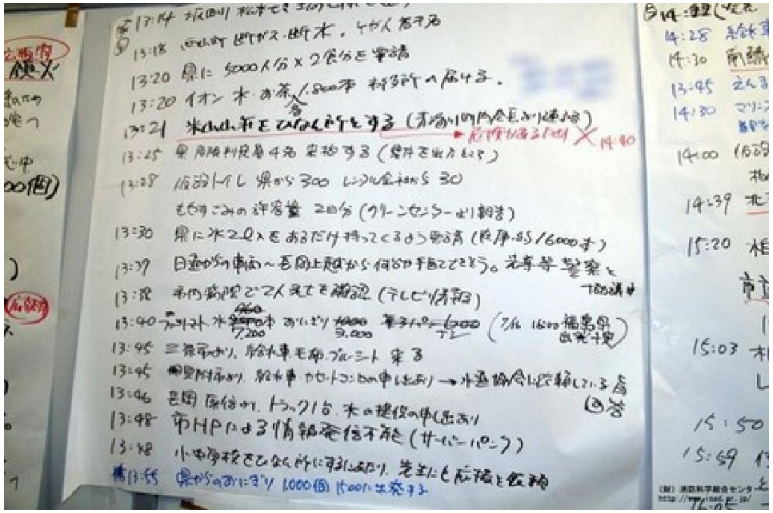
アナログでOK
目的達成が肝要！

実際の対策本部の様子



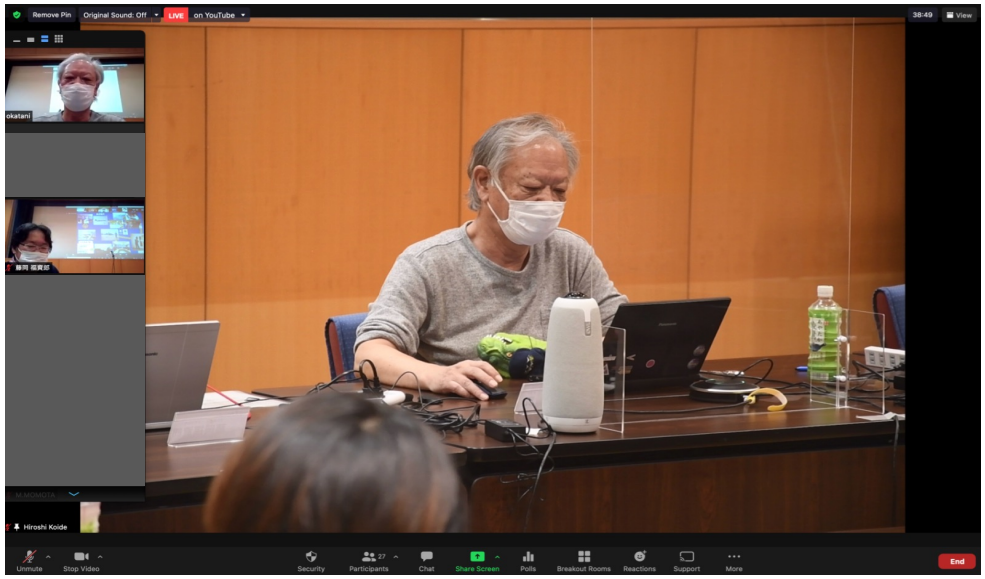


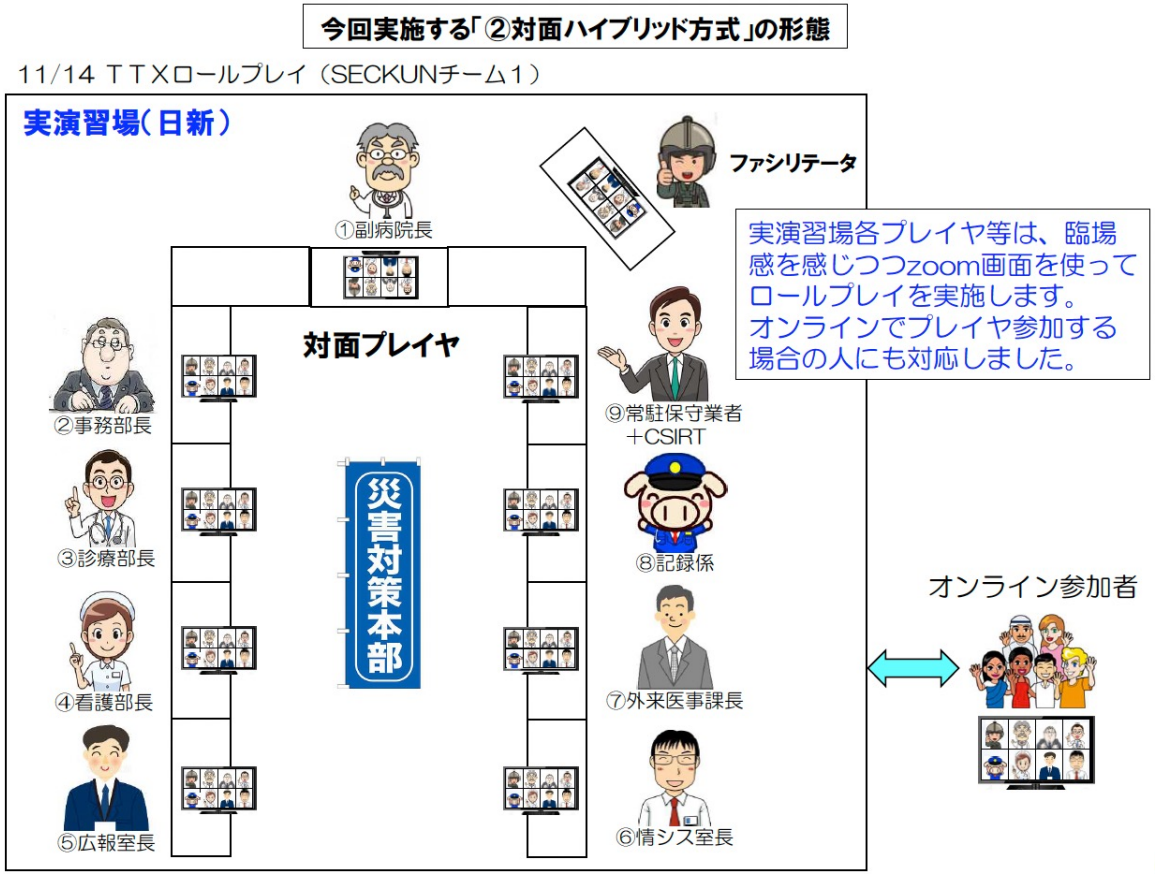




目的指向！

九大におけるTTXの実施例（2021/11/14）





九大におけるTTXの実施例（2020）

Zoomオンライン参加者画面

簡易防護服装着体験

進めやすい！適切な「状況付与」

TTXシナリオ　（1）初動段階及び判断対応段階（エスカレーション）ステージ1

【状況付与】

朝、当直医が電子カルテ端末をチェックしようとすると….

もしもし、当直医ですが。
電子カルテ端末に変な画面が出て、使えないんですが。

確認して貰えますか。

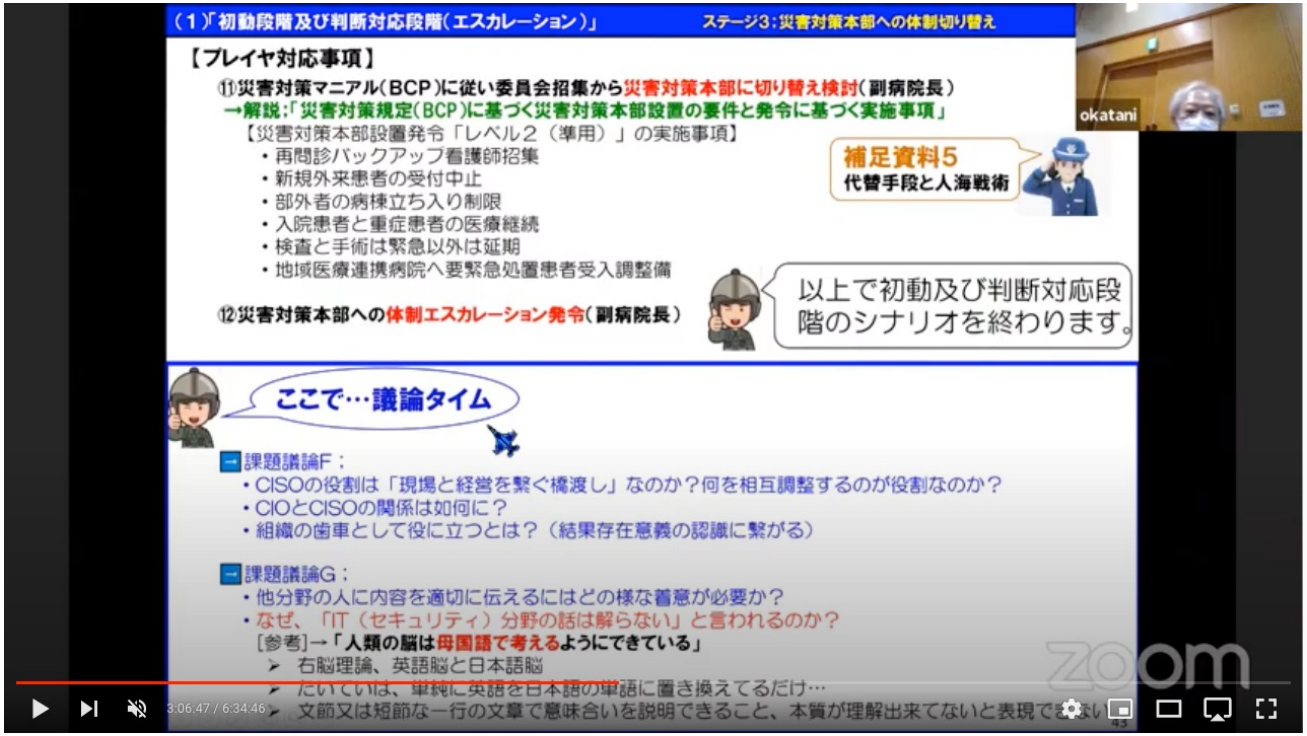
○当直医

⑥情シス室長

はい、解りました。
直ちに、常駐保守業者と向います。

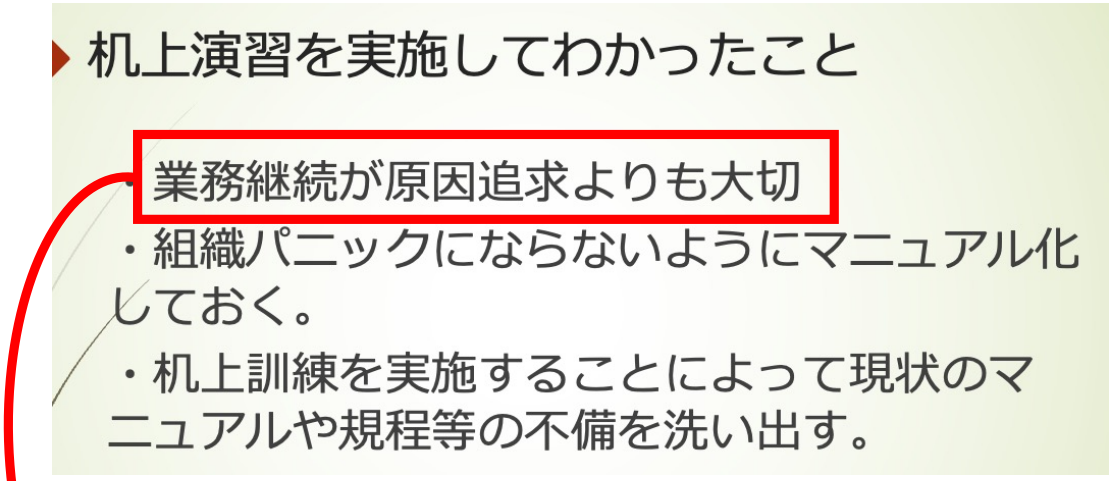
ときどきはいる「議論タイム」！

- Roleplay でファシリテータにより有益な知見が得られる重要な局面で「議論タイム」が入れられる
- 参加者が得た気づきや重要事項を共有
- より深く考えるきっかけとなる



まとめ

- 組織におけるミッションを達成するために事業継続を行うための事前準備のための机上演習について紹介
- 九州大学のProSec-IT/SECKUNで行われているBCP体験型机上演習について紹介
- 事業継続のためには120パーセントの準備が大事！



受講生の声（最終成果報告のスライドから引用）

この受講生は当然良く理解できているが．．．それでもITセキュリティ分野の人たちは原因追求がしたくなる．．

「まず応急処理を行い事業継続対処を行ったあとに事態が沈静化してから原因調査を行う」のが良い

本TTXでは、組織BCP事態対処場面における「原因追跡の意義」を全体的視点から考えます