中小製造業向け
体験型演習の概要紹介

令和5年2月1日（水）15:00-17:00

九州大学サイバーセキュリティセンター
小出　洋

サイバー攻撃を受けたら・・・

生産停止する工場ですか？
生産継続できる工場ですか？

サイバー
セキュリティ
×BCP

工場の緊急時生産管理体制を共に考える！

「中小製造業向け体験型演習」
開催に向けた事前説明セミナー

令和５年
２月１日(水)

15:00～
17:00

オンライン
(Microsoft Teams)

参加費無料

【プログラム】

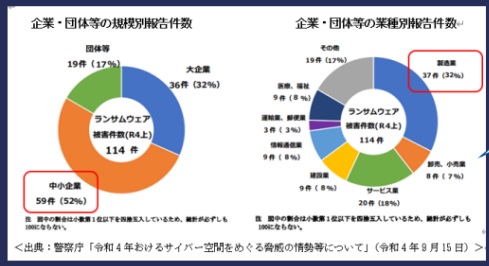
1　中小製造業を巡る情勢とセキュリティ･BCP関連施策のご紹介　【九州経済産業局】

2　中小製造業向け体験型演習の概要紹介　【九州大学】

3　工場セキュリティハンドブックのご紹介と演習との相乗効果について　【日本ネットワークセキュリティ協会】

4　パネルセッション　～企業目線の解説～　【九州大学、マツダ(株)、(株)安川電機】

主催：経済産業省九州経済産業局、九州大学サイバーセキュリティセンター、一般財団法人九州オープンイノベーションセンター
後援（予定）：JNSA（NPO法人日本ネットワークセキュリティ協会）



＜出典：警察庁「令和４年おけるサイバー空間をめぐる脅威の情勢等について」（令和４年９月15日）＞

警察へのランサムウェア**被害報告件数の52%が中小企業**、業種別では**製造業が最多**。

不正アクセスといったサイバー攻撃が**“引き金事象”**となって工場が機能不全に陥り、生産停止や保安事故などが起こると、製品の生産・出荷に支障をきたし、取引先との関係のみならずサプライチェーン全体にも影響が出ることが昨今強く懸念されています。

とはいえ、日々攻撃の手口が巧妙化するなか、工場へのサイバー攻撃による生産への影響を完全にゼロにすることはできませんが、**自然災害による被害と同様に、重要視すべきは“生産の継続（BCP）”ができるように備えること**です。

今回実施する演習は、九州大学が社会人向け実践教育プログラムの一つとして実施されていたプログラムを、**“中小製造業向け”にアレンジし提供する“全国初”の取組**となります。

サイバー攻撃による生産設備等の機器障害発生時における対策本部活動、緊急生産管理体制等を予め検討し訓練を行い、影響を最小限にするための**課題・対応を共に考えませんか？」**

○申し込み方法
下記フォームよりお申し込みください。入力できない場合はメールで、
①企業・団体名、②所属部署、③役職、④氏名、⑤メールアドレスを
九州経済産業局デジタル経済室（kyushu-iot@meti.go.jp ）までご連絡ください。
URL：https://mm-enquete-cnt.meti.go.jp/form/pub/kyusyu-johoseisaku/ttx-seminar
○申込締切：令和５年１月３０日（月）１８：００
○登壇者等詳細はこちら：https://www.kyushu.meti.go.jp/event/2301/230110_2.html

○お問い合わせ先：経済産業省　九州経済産業局　デジタル経済室　担当：春口、横尾
TEL：092-482-5552　E-mail：kyushu-iot@meti.go.jp

○個人情報取り扱いの方針
ご提供いただいた個人情報は、事務局（九州経済産業局、九州大学サイバーセキュリティセンター、一般財団法人九州オープンイノベーションセンター）及び講師が、本事業（「中小製造業向け体験型演習」開催に向けた事前説明セミナー）の運営においてのみ使用し、事務局においてその保護について万全を期すとともに、ご本人の同意なしに事務局及び講師以外の第三者に開示、提供することはございません。オンライン形式（Microsoft Teams）では、入室時に設定した登録名が画面に表示されます。個人情報保護の観点から、「中小製造業向け体験型演習」開催に向けた事前説明セミナー」当日は、公表可能な名称を設定してください。（ご参加いただくための入室用URLをお知らせする際にも、改めてご案内いたします）。

小出　洋（こいで　ひろし，Hiroshi Koide）

JavaOne2009 SunSPOT BOFにて

Twitter　@hirosk
Facebook　Hiroshi Koide
YouTube　@koide55

経歴

電気通信大学大学院博士後期課程修了
↓
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
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 (Social Contribution)

- ☆ SECCON実行委員, SECCON executive committee
- ☆ IPA セキュリティ・キャンプ in 福岡,

得意分野 (My Interests)

- ☆ プログラミング, Programming
- ☆ サイバーセキュリティ, Cyber Security

（Moving Target Defense, 脅威トレース(Simulation System of Malware and Information Systems)…）

Awards

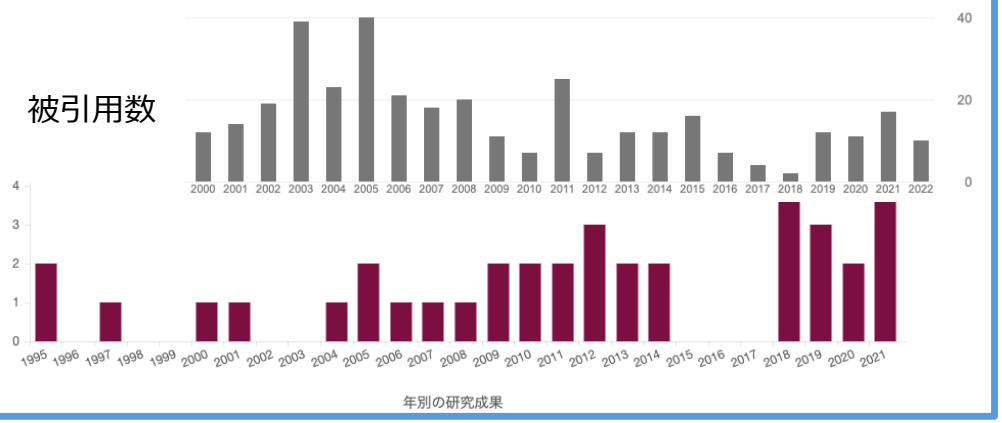
- ☆ IPA スーパークリエータ, IPA MITOH Super Creator
- ☆ JavaOne 2005 Duke’s Choice Award
- ☆ Sun Microsystems Center of Excellence

Overview of Hiroshi Koide

研究内容

Moving Target Defense
- サイバーセキュリティ
- 情報システム
- IoT
- サイバー攻撃

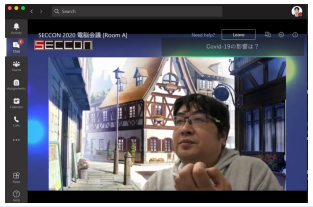
年別の
研究成果



佐賀県警サイバー犯罪
対策技術アドバイザ
2022.9.16 ～

福岡県警サイバー犯罪対策
テクニカルアドバイザ
2014.10.28 ～

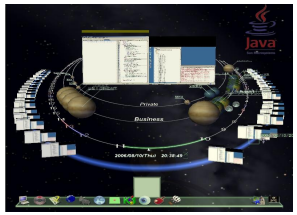
SECCON実行委員
2012.3 ～



Twitter @hirosk
Facebook Hiroshi Koide
YouTube @koide55

Duke’s Choice Award
2005.6.28

IPA未踏ソフトウェア創造事業
スーパークリエータ認定
2006.10.24

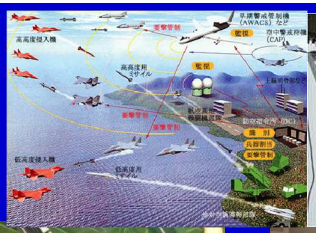


今日これから紹介する体験型演習を一言で

- サイバー攻撃を受けて守れなかったときどうする？
- 体験型演習で模擬体験＝イザというときに焦らないで済む
  （演習は考える訓練）
- 実際の緊急対応を正確に反映したシナリオで模擬体験
- 大事なのは生産継続（フェイルセーフ＝壊れても大丈夫！）
- サイバー攻撃は引き金事象
  ＝生産継続のために緊急生産管理対応オペレーションが軸
- 体験型演習で以下の全過程をカバー
  予防整備～緊急生産管理体制～再発防止策検討
- シナリオは考えるための思考ひな形
  回を重ねる度に演習シナリオは集合知により成長

岡谷 貢 隊長

自己紹介



JASDF

防衛省 MINISTRY OF DEFENSE

社会貢献活動

富士通特機安保研
IPA専門委員
JNSA
IIJアドバイザ
島根県警TA
九州大学教官
各種政府等支援

今日これから紹介する体験型演習を一言で

- サイバー攻撃を受けて守れなかったときどうする？
- 体験型演習で模擬体験＝イザというときに焦らないで済む
  （演習は考える訓練）
- 実際の緊急対応を正確に反映したシナリオで模擬体験
- 大事なのは生産継続（フェイルセーフ＝壊れても大丈夫！）
- サイバー攻撃は引き金事象
  ＝生産継続のために緊急生産管理対応オペレーションが軸
- 体験型演習で以下の全過程をカバー
  予防整備～緊急生産管理体制～再発防止策検討
- シナリオは考えるための思考ひな形
  回を重ねる度に演習シナリオは集合知により成長

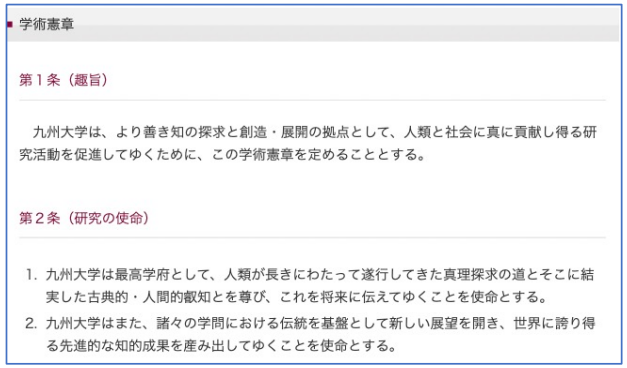
組織におけるミッション

- 組織にはそれぞれの役割・ミッションを持つ
- ミッションが組織の存在意義・使命

例）

- Googleのミッション（Google's mission is **to organize the world's information and make it universally accessible and useful**.）
- 九州大学のミッション（研究・教育・医療）
- 病院（それぞれの病院に応じた役割）
- **製造業（社会に必要な製品を製造；社会インフラとして役割）**

組織ミッションを継続し，遂行することがその存在意義
組織はそれにより社会に貢献



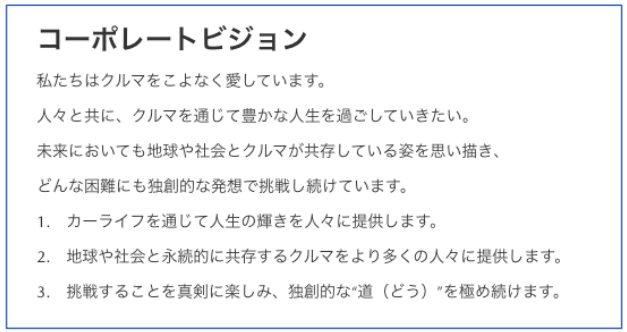
学術憲章

第１条（趣旨）

九州大学は、より善き知の探求と創造・展開の拠点として、人類と社会に真に貢献し得る研究活動を促進してゆくために、この学術憲章を定めることとする。

第２条（研究の使命）

1. 九州大学は最高学府として、人類が長きにわたって遂行してきた真理探求の道とそこに結実した古典的・人間的叡知とを尊び、これを将来に伝えてゆくことを使命とする。
2. 九州大学はまた、諸々の学問における伝統を基盤として新しい展望を開き、世界に誇り得る先進的な知的成果を産み出してゆくことを使命とする。



コーポレートビジョン

私たちはクルマをこよなく愛しています。

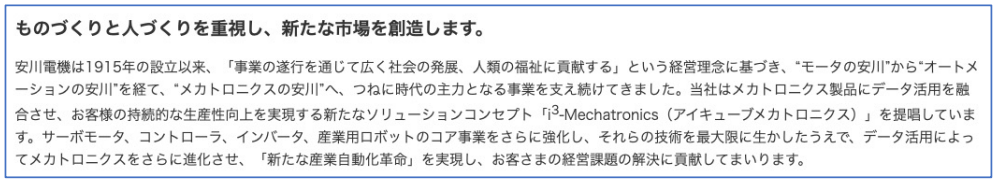
人々と共に、クルマを通じて豊かな人生を過ごしていきたい。

未来においても地球や社会とクルマが共存している姿を思い描き、

どんな困難にも独創的な発想で挑戦し続けています。

1. カーライフを通じて人生の輝きを人々に提供します。
2. 地球や社会と永続的に共存するクルマをより多くの人々に提供します。
3. 挑戦することを真剣に楽しみ、独創的な“道（どう）”を極め続けます。

マツダのコーポレートビジョン
https://www.mazda.com/ja/about/vision/



ものづくりと人づくりを重視し、新たな市場を創造します。

安川電機は1915年の設立以来、「事業の遂行を通じて広く社会の発展、人類の福祉に貢献する」という経営理念に基づき、“モータの安川”から“オートメーションの安川”を経て、“メカトロニクスの安川”へ、つねに時代の主力となる事業を支え続けてきました。当社はメカトロニクス製品にデータ活用を融合させ、お客様の持続的な生産性向上を実現する新たなソリューションコンセプト「i^3-Mechatronics（アイキューブメカトロニクス）」を提唱しています。サーボモータ、コントローラ、インバータ、産業用ロボットのコア事業をさらに強化し、それらの技術を最大限に生かしたうえで、データ活用によってメカトロニクスをさらに進化させ、「新たな産業自動化革命」を実現し、お客さまの経営課題の解決に貢献してまいります。

安川電機の経営理念
https://www.yaskawa.co.jp/company

組織のミッション継続をさまたげる要因

さまざまな外的・内的要因（引き金事象）が存在している

- テロ，自然災害
- 不祥事，内部犯罪
- 社会情勢
- 情報システムに関連する大規模障害
- 情報システムに対するサイバー攻撃

- 事業継続を妨げるという視点では「情報システムに対するサイバー攻撃によるシステム障害」と他の要因の違いはあまりない
- どの要因も完全に防ぐ方法は無いが，対策が不要というわけではない

サプライチェーンに対する攻撃

- 特定の企業グループ，関連会社，取引先全体を通じ，工業製品などの原料や部品の一連の流れ（サプライチェーン；供給連鎖）に対して行われる攻撃
- 企業が持つ機密情報の窃取やランサムが目的（10大脅威の3位）
- サプライチェーンのなかでもっとも弱い中小企業などがターゲットとして狙われ，攻撃されるとそこを踏み台として大企業も攻撃

- サイバー攻撃はソフトウェアの更新やパスワードの管理などの情報技術に関連する基本的な対策を実施しても100パーセント防げない

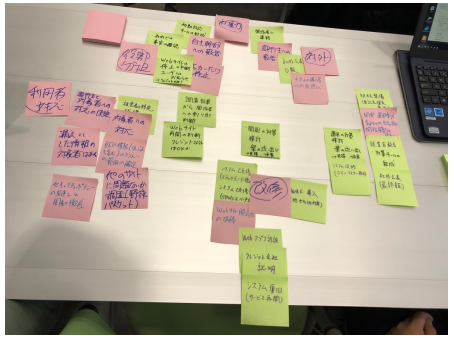
（テロや不祥事，社会情勢などの要因と同様）

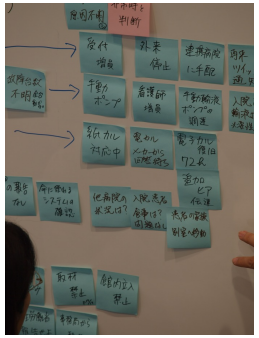
- 攻撃が防げなかった万一の事態に備えた緊急生産管理体制の計画が必要

体験型演習のイメージの共有

体験型演習とは？

- 実際に近いロールプレイ形式で具体的かつ実際的なシナリオを用いる模擬演習
- そのシナリオにより対処が必要な緊急事態を模擬体験
- 「オリエンテーション」「非常訓練」というイメージが近いです
- 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で対処の余裕が生まれる





体験型演習のイメージの共有

体験型演習とはどのようなものかイメージを共有するために．．．

- まず先行して開発されて完成度が高い「事業継続計画（BCP）体験型演習（医療継続シナリオ）」を紹介します

- 医療継続シナリオは，今回試行する「中小製造業向け体験型演習」とは異なりロールプレイも含まれています
  - BCP体験型演習（医療継続シナリオ）＝　ロールプレイ＋ディスカッション
  - 中小製造業向け体験型演習　＝　現段階ではディスカッション中心

- これから議論と研究を重ねながら中小製造業向け体験型演習をより精度の高い（ロールプレイも含む）有益な体験型演習にしていきます

医療現場で電子カルテシステムにランサム被害（例）

奈良宇陀市立病院 2018.10

徳島つるぎ町立半田病院　2021.10

大阪急性期・総合医療センター　2022.10

体験型演習の目的

事業継続計画（BCP）

- 既存の緊急対処計画（緊急時生産管理計画BCP/BPM；医療安全管理マニュアル）をベースにサイバー攻撃が引き金事象となった場合を追加したもの

事業継続計画（BCP）の検証

- BCPを作成しただけでは不十分．それに伴う体制の検証が必要
- 想定外のことがおきるかもしれず，想定外のことは準備できない
- 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）
- 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）

医療シナリオの体験型演習（2019）

岡谷貢隊長

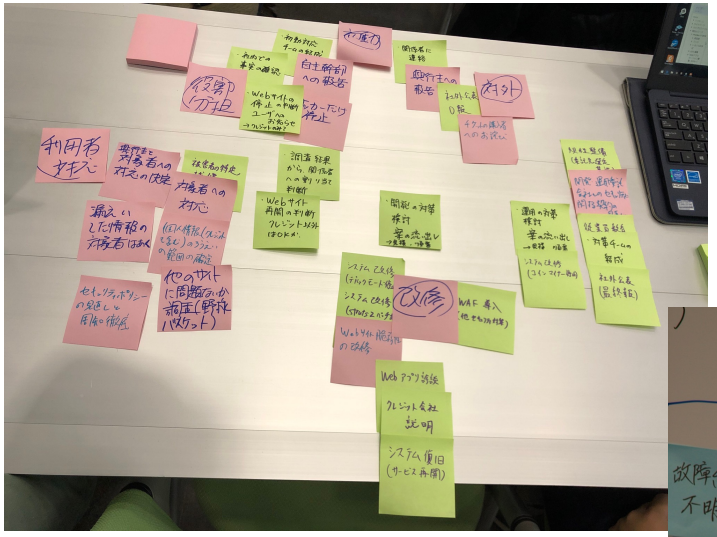
TTX・・・Table Top eXercise（机上演習）

詰める・詰められる・エクササイズ

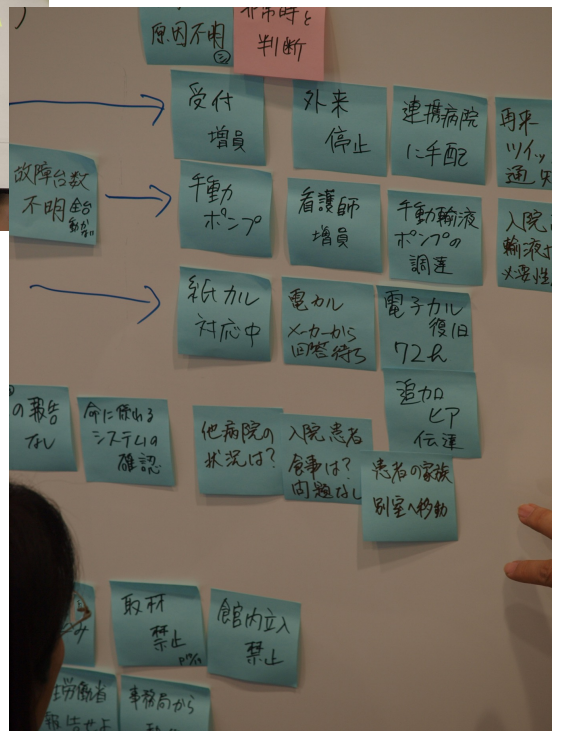
→計画やルールに不備はないか、実戦形式でチェック

※受講生の最終成果報告会のスライドから抜粋

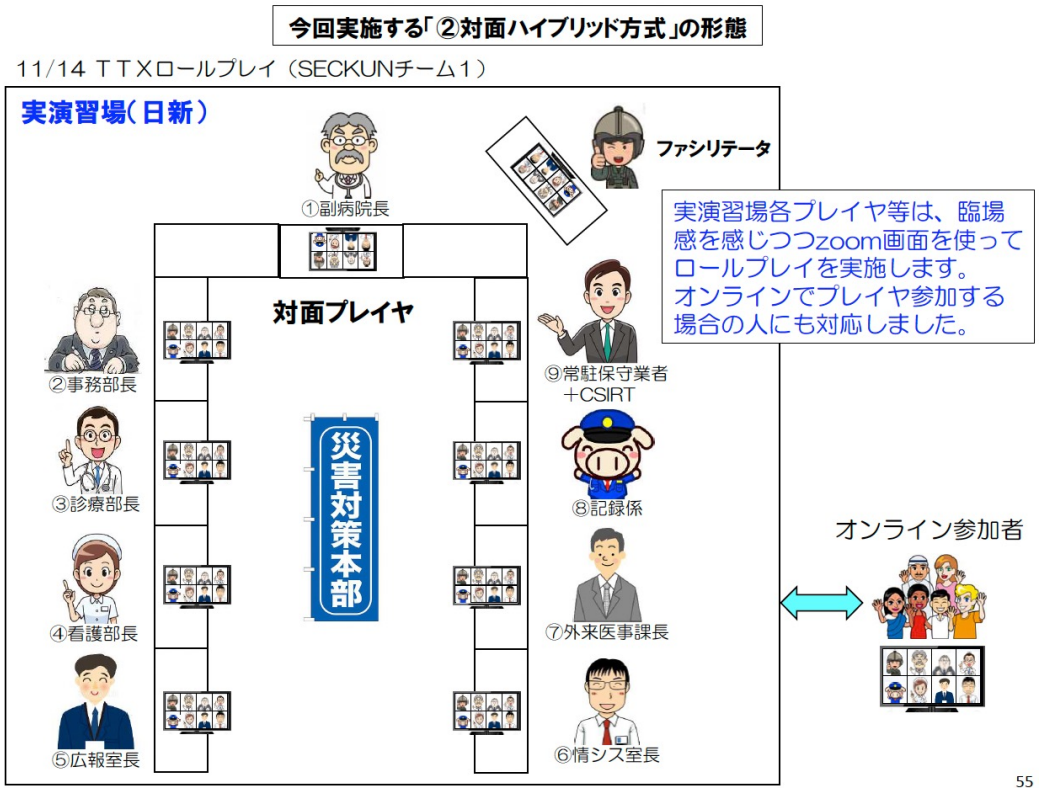
医療シナリオの体験型演習 （2019）



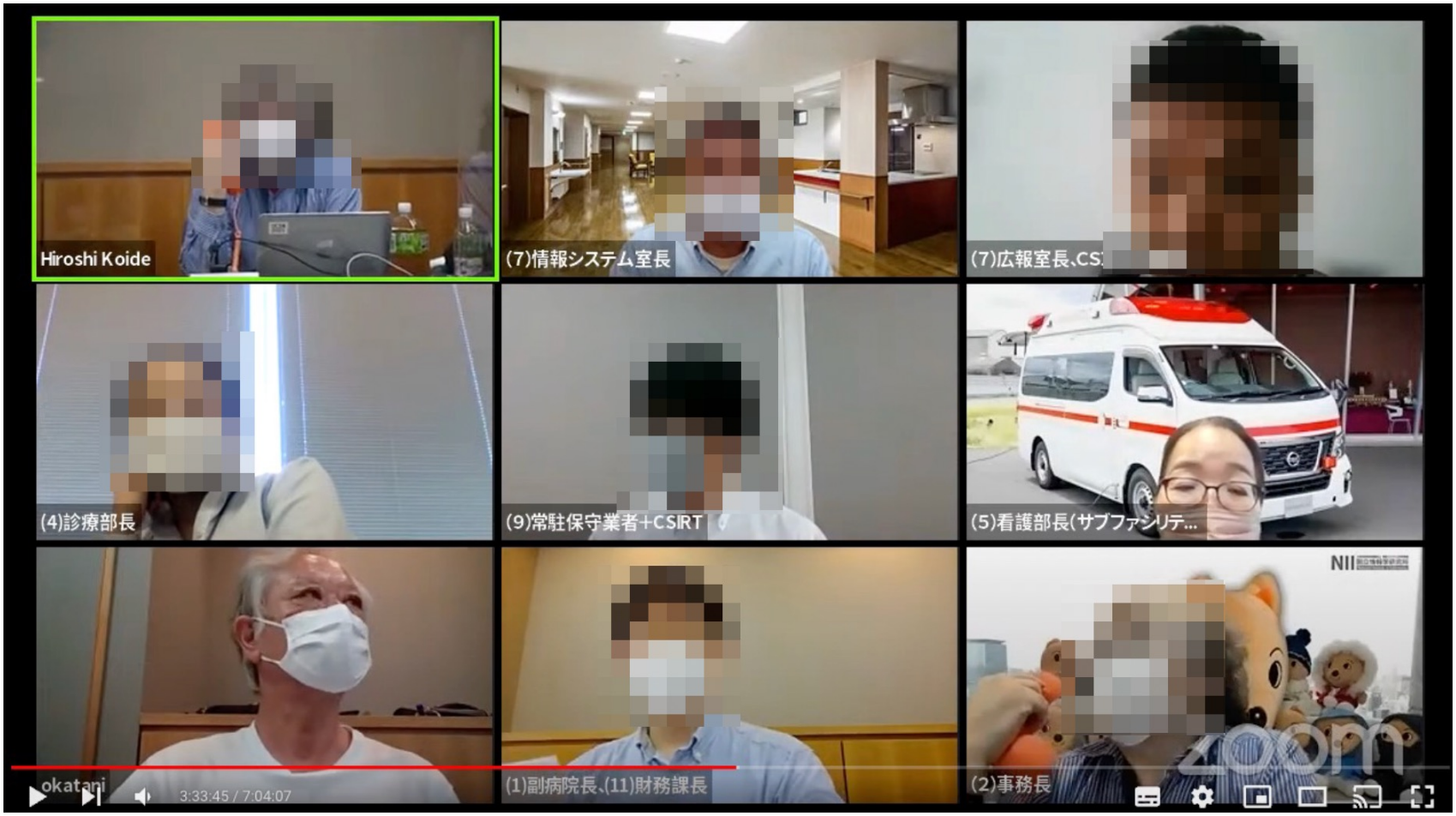
アナログでOK
目的達成が肝要！



医療シナリオの体験型演習　（2021）

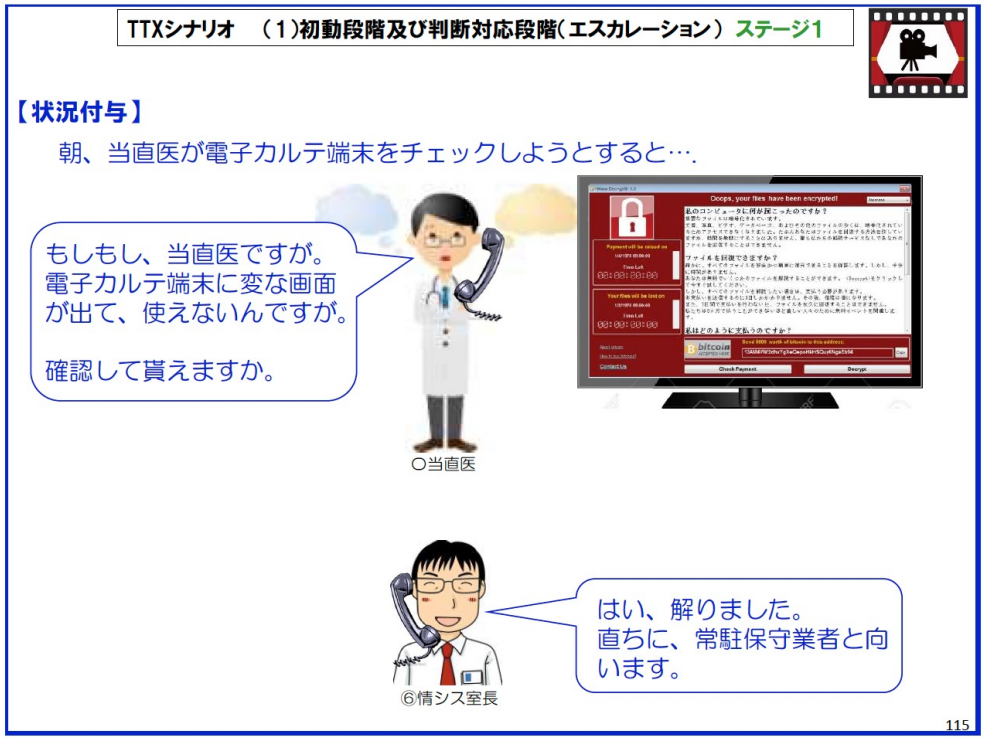


医療シナリオの体験型演習（2022/10/01）

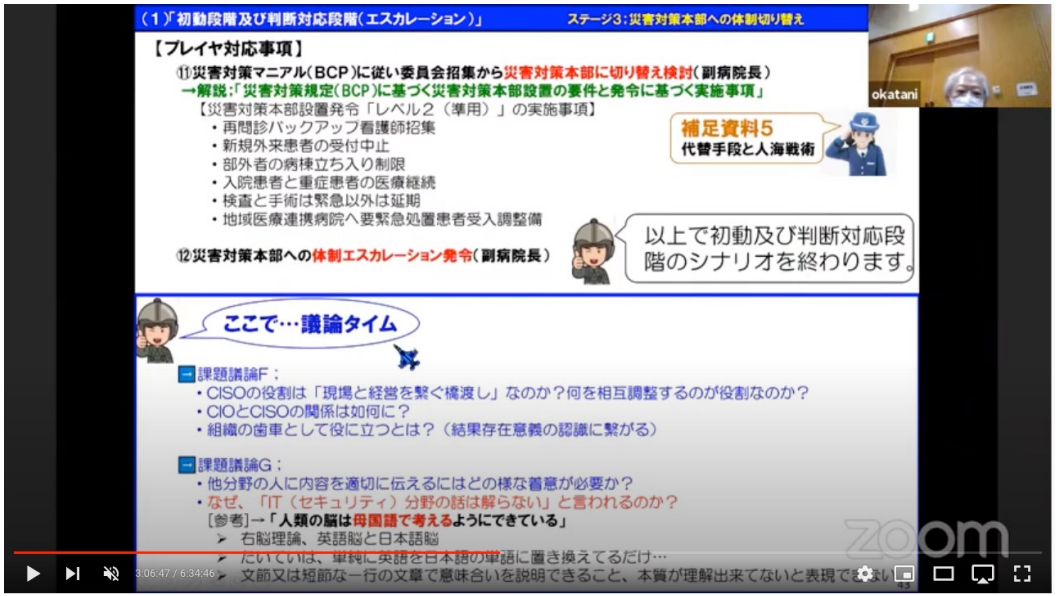


フルオンライン

進めやすい適切な「状況付与」やときどき入る「議論タイム」



進めやすい適切な「状況付与」



- ロールプレイ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」が設定されている
- 参加者が得た気づきや重要事項を共有しより深く考えるきっかけとなる

ときどき入る「議論タイム」

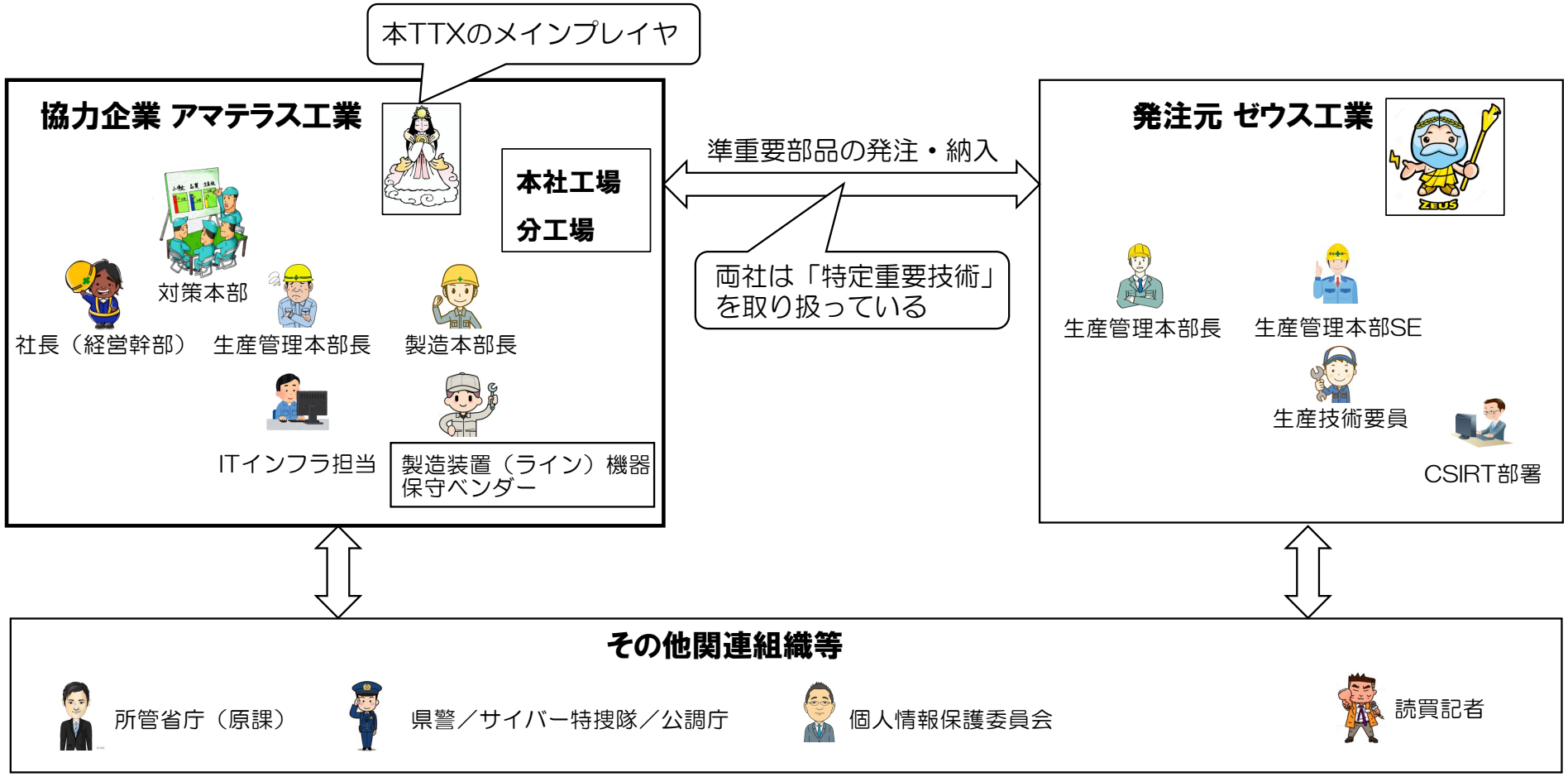
中小製造業向け体験型演習
シナリオのイメージの共有

体験型演習規定

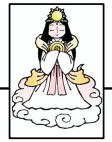
本TTX(＝体験型演習)シナリオ設計の基本的考え方

- 本シナリオの設計コンセプトは「**予防整備的対策で守れなかった(防げなかった)らどうする？を考えてBCM(緊急生産管理計画)手順を考えておく**」事の重要性を理解する事にある。
- 本シナリオで想定するサイバー攻撃の種類と意義は以下。
  →サイバー攻撃の影響カテゴリは複数、本シナリオでは「**機器障害が生産継続に影響を及ぼす場合**」とする。
- 研究TTXは具体的事例を提示してBCM計画を考えるのが目的。これにより、各部署の論点イメージを一致させる。
  →**演習は考える訓練！シナリオは思考ひな型！**
- 対応基準やマニアル作成を目的とする場合はあらゆる原因を前提に整理していくが、最初からこれで考え始めると対応軸が掴めず具体策検討に繋がりにくい。TTXとは目的が別。
  →TTXは、**対応マニアルや基準作成が目的ではなく**、これらを部門連係下で**検討するための土俵作り**となる。
- シナリオは現実想課題状況に則した内容とするため、現象が具体的に見える脅迫型ランサムウエア（Lockbit2.0）事例を基にしつつも**より対応が難しい製造ライン障害を加味したサイバー攻撃内容**（LB2.0仕様の脅迫型ランサムウエア＋α）とする。
- 架空の企業と対応内容を題材に構成し、本資料内容の保全性を図る。
- 今回は、製造業分野最初のTTXシナリオとなる。このため重要論点を絞ったシナリオとする。
  →TTX**課題議論の中で様々なケースを検討**し意見集約を図る。
- シナリオではAB２種類の攻撃パターンを想定するが攻撃手法は常に変化するため攻撃手法毎の対策検討では際限なく対処手順変更を行う事になる。このため生産管理への影響部分に重点を置き、**攻撃手法に共通的な対応内容を対応手順(BCM)化**する事を想定したシナリオとした。
- 各ステージで**演習課題を基に模擬討論(研究型TTX)を行う。**課題は予め準備したものの中から**参加プレイヤの属性に応じてセット**する。
  →演習課題の中にプレイヤ気づき事項とメッセージを込める（このため**プレイヤ属性に応じ課題内容を変える**）。

演習関連組織相関図


本TTXのメインプレイヤ
協力企業 アマテラス工業
本社工場
分工場
準重要部品の発注・納入
両社は「特定重要技術」を取り扱っている
発注元 ゼウス工業
対策本部
社長（経営幹部）
生産管理本部長
製造本部長
ITインフラ担当
製造装置（ライン）機器保守ベンダー
生産管理本部長
生産管理本部SE
生産技術要員
CSIRT部署
その他関連組織等
所管省庁（原課）
県警／サイバー特捜隊／公調庁
個人情報保護委員会
読買記者

演習組織想定



協力企業 アマテラス工業

- ITインフラ担当は生産管理部に所属
- 製造本部、生産管理本部、情報管理系のネットワークとサイバー機器等を管理→ITインフラシステム管理担当等（ITインフラ担当）
- ITインフラ担当が管理する機器の上で動作する運用プログラム管理は各所管部等が担当
- BCMは、ISO22301（JIS）を根拠とし、IATF等の基準も参考に**自社BCM（緊急生産管理計画）を作成**している。
  →IATFの緊急事態対応計画の想定事態等
- 発注元と定期的に**BCM勉強会を実施**している。
- 発注元との資本関係はない→生産管理データの連携性は疎
- 生産管理データの連携性は疎のため、SSLでデータ交換。EDIでの受発注データが主
- 製造に必要な数値情報等（受発注データ等）は、発注元～協力企業間で予め取り決めてある
- 社内本社工場～分工場間は、社内EDIシステム間をSSLでデータ交換
- 生産管理システムは**バッチバックアップを取っている。ただし、フルレストアの訓練は行っていない。**
- 経済安保推進法による「**特定重要技術**を扱う事業者（所管大臣指定）」の**対象となる技術を用いた製品を製造し、発注元企業に納入**している。


対策本部


社長（経営幹部）


生産管理本部長


製造本部長


ITインフラ担当


製造装置（ライン）機器保守ベンダー

・組織図

協力企業 アマテラス工業

商号	㈱アマテラス工業
設立	1950年（昭和25年）4月20日
資本金	8,000万円
従業員数	157名（2023年1月現在）

社長（経営幹部）

株主総会

取締役会

会長・社長

役員会

監査役

経営企画室

総務部

経理部

営業本部

営業部

調達部

生産管理本部

生産管理本部長

技術技術部

生産管理部

ITインフラ担当

ITインフラ担当

品質保証部

製造本部

製造本部長

本社工場

分工場

設備環境部

発注元 ゼウス工業

- BCMは、ISO22301（事業継続）を準拠とし、JTAS等の基準も参考に**自社BCM（緊急生産管理計画）を作成**している。
  →JTASの緊急事態対応計画の想定事態等
- 協力企業からは**「準重要部品であり、代替が利く部品」の納入**を受けている。→**代替メーカから入手可**
- 準重要部品は、**常時2週間ぶんの在庫確保**しているものとする。
- サイバー攻撃対処の**専門部署（CSIRT）を持っている**
- 経済安保推進法による「特定重要技術を扱う事業者（所管大臣指定）」であり、研究開発にあたり指定基金（経済安保重要技術育成プログラム）の認定を受けており、**社内に「特定重要技術」情報を保有**している。


生産管理本部長


生産管理本部SE


CSIRT部署


生産技術要員

その他関連組織等；

- 国県関係者
  個人情報保護委員会、業法所管部署、警察等、報道、関係ベンダー等
- 関係省庁等は次を想定する。
  「製造安全関連所管省庁」「個人情報保護委員会」「経済安保関連所管省庁」「県警本部及び警察庁サイバー特別捜査隊」「公安調査庁」


所管省庁（原課）


県警／サイバー特捜隊／公調庁

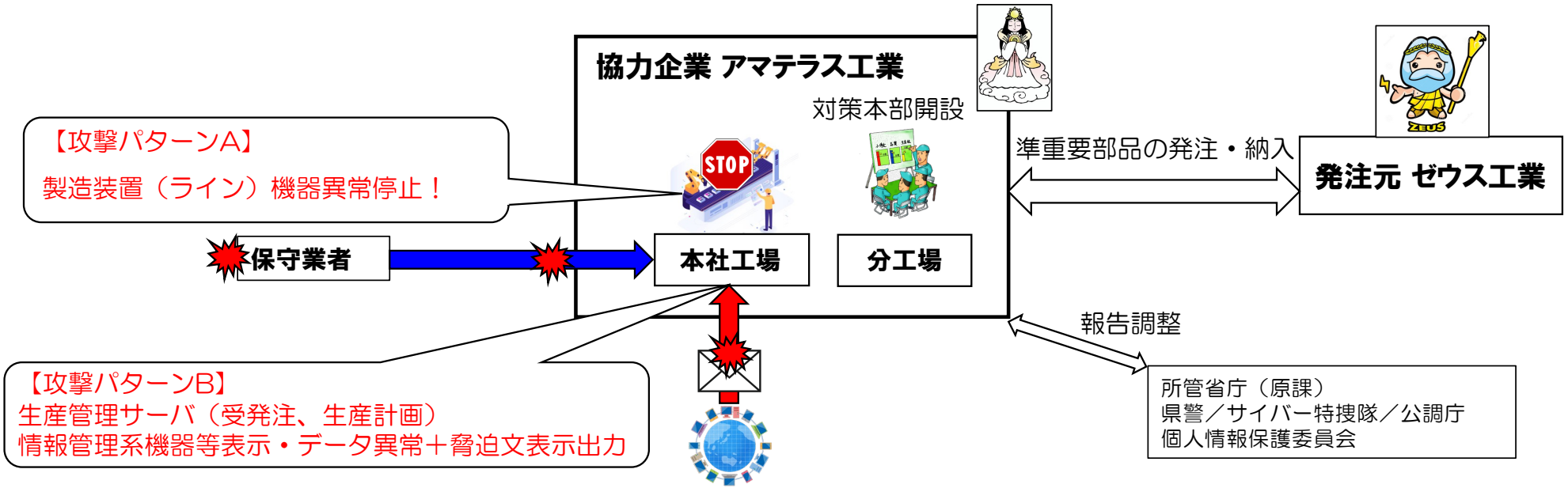

個人情報保護委員会


読買記者

演習状況概要

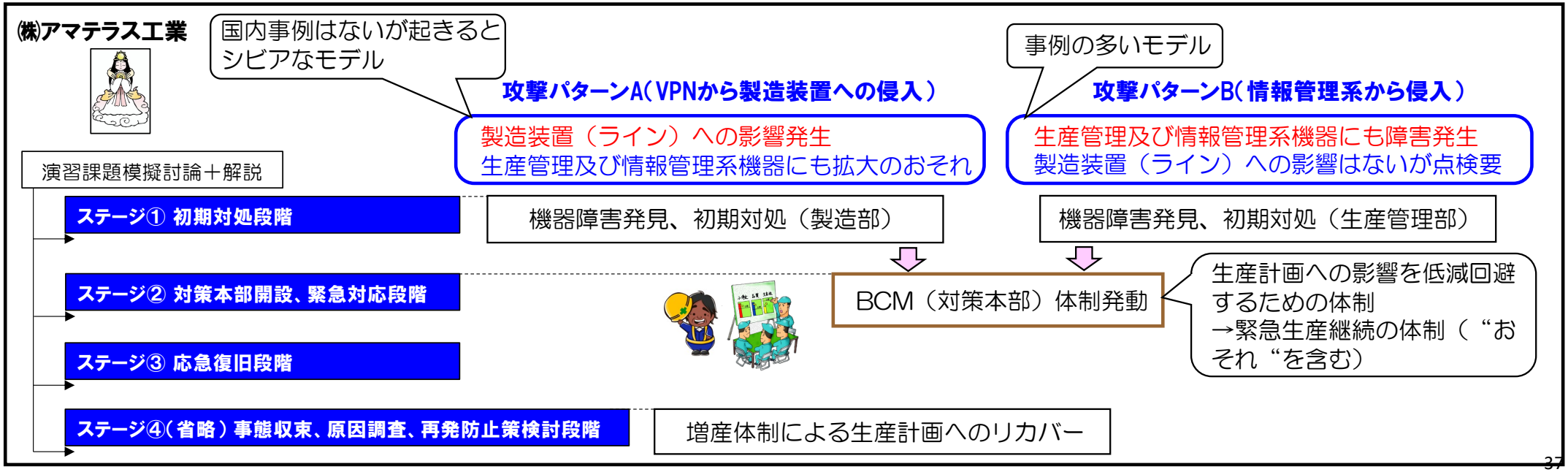
本演習シナリオは、実際に起きた事例を基に対策本部体制で対応するであろう事態対処事項を可能な限り忠実に再現した。
「サイバー攻撃を引き金事象とした製造業緊急生産管理体制（BCM）の検討」に関し、各所検討場面における「思考ひな型」としての活用を想定して作成したものである。

協力企業アマテラス工業はサイバー攻撃を受けた。シナリオで設定する攻撃パターンは２種類。
パターンAでは保守業者との保守用VPN接続部から侵入、製造装置（生産ライン）が異常停止。製造部はオンコールを実施障害対応を行う。
パターンBではインターネットからの標的型メールにより情報管理系機器に侵入し表示及びデータ異常により運用不能。
アマテラス工業はBCMに基ずく対策本部を設置。緊急生産管理体制を取り、関係各所への報告調整並びに被害状況の把握と応急復旧を検討する。製造装置（生産ライン）は点検停止する。
対策本部は、生産継続への影響を極小化し速やかな生産再開を目指す。



【シナリオ概要】
製造業であるアマテラス工業の本社工場に脅迫型ウイルスによるサイバー攻撃が発生した！
攻撃パターンはAB２種類の場合を想定、それぞれ製造装置（ライン）及び生産管理系情報管理系機器に障害が発生し製造及び機器運用不能な状態となる。
一方の攻撃パターンAでは生産装置（ライン）が自動停止、製造部からの保守業者オンサイトコールによる対処が行われる。
アマテラス工業は生産継続（発注元であるゼウス工業への部品納入）への影響がある事態と判断、社内全システム停止を指示。
同時に、BCMに基ずく対策本部を設置し、部品納入先である発注元ゼウス工業と連携し生産継続のための緊急対応オペレーションに入った。

アマテラス工業はBCMを参考に応急復旧手順を開始、生産継続への影響を極限する対応を行い速やかな応急復旧処置と最低限の生産再開を図る。
爾後、増産体制による生産計画へリカバーし、生産計画への影響は回避された。



【シナリオサマリ】

パターンA（VPNから製造装置への侵入）

各対応項目は協力企業 アマテラス工業 の対応内容

ステージ① 初期対処段階

A②保守会社オンコール

A③ITインフラ担当初期確認開始

BCM（対策本部）体制発動
○各関連部署が対応に動き出す
○緊急生産継続オペレーション開始

以降、パターンA、B共同じBCMプロセス

製造本部

A①製造尉装置（ライン）の一部に機器障害発生確認、初動対処

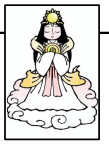
STOP

製造装置（ライン）機器

生産管理装置（ライン管理端末）

保守業者

協力企業 アマテラス工業



生産管理部所属のITインフラ係が機器管理
→ITインフラ部分

生産管理本部

A④他生産管理装置の状況確認（おそれ有）

MESサーバ（製造実行システム）

A①には２種類の状況発生がある
- 製造装置（ライン）の異常停止
- MES（製造実行システム）端末の表示異常等
  →脅迫画面表示＆データ異常

その他部署
- 営業
- 調達
- 品質管理　等

生産管理サーバ（受発注、生産計画）

A⑤情報管理系機器の状況確認（おそれ有）

情報管理系機器等

状況補足解説；

○一番クリティカルなケース
- **製造装置（ライン）の機器異常発生→歩留まりモニター表示異常、ライン自動停止等→製造部は初期対処**
- **機器異常から状況スタート（表示異常ではない）、製造部としては通常のオンコールに向かうシビアなケース**

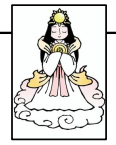
○製造系にADは無いのでMES等に伝搬はせず（LB2.0の場合）、生産管理装置、情報管理系に影響無とする。
- **→影響無でも生産管理本部は「念のため」A④⑤での確認を行う。**
- **→本TTXの論点はBCM手順の検討であるため、課題議論の中で「影響有」の場合の対応も議論する（LB2.0に限らず）**

【シナリオサマリ】

パターンB（情報管理系から侵入）

ステージ① 初期対処段階

各対応項目は協力企業 アマテラス工業 の対応内容



協力企業 アマテラス工業

製造本部

製造装置（ライン）機器

保守業者

生産管理装置（ライン管理端末）

生産管理部所属のITインフラ係
が機器管理
→ITインフラ部分

生産管理本部

MESサーバ（製造実行システム）

B③製造部への影響確認

B②ITインフラ担当初期確認開始

B①情報管理系機器に機器障害発生（LB2.0の場合は目視で気づく）
＊LB2.0は、アクティブディレクトリーサーバ情報を参照し自立拡散

その他部署
- 営業
- 調達
- 品質管理　等

生産管理サーバ（受発注、生産計画）

情報管理系機器等

標的型メール

インターネット

BCM（対策本部）体制発動
　〇各関連部署が対応に動き出す
　〇緊急生産継続オペレーション開始

以降、パターンA、B共同じBCMプロセス

状況補足解説；
〇良くあるパターン。
〇製造機器に影響はないが、生産管理システムには影響が発生（表示＆データ異常で発見）し、結果としてラインを点検停止する。

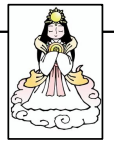
【シナリオサマリ】

BCM（対策本部）体制発動
　〇各関連部署が対応に動き出す
　〇緊急生産継続オペレーション開始

パターンAB共通

各対応項目は協力企業 アマテラス工業 の対応内容

協力企業 アマテラス工業



ステージ② 対策本部開設、緊急対応段階

C① **対策本部設置**、各部門の状況確認指示
C② 生産管理本部は**生産ラインの停止を検討**
C③ 生産管理本部は**経営幹部と営業へ生産ラインが止まる事を連絡**
C④ **経営幹部は生産ラインの停止を決心**
C⑤ **営業部門は発注元への連絡（納期遅延、生産停止等）**
C⑥ **BCMに基づく初期対処事項を実施**

点検含め生産ラインを止める！

対策本部活動で生産への影響を最小化する！

ステージ③ 応急復旧段階

C⑦ **各部署被害見積もり**
C⑧ 工場含む社内**全システムの停止を指示**
C⑨ 生産ラインとの**分離可否と影響の有無を調査**
C⑩ **応急復旧計画と再稼働見積もり**
C⑪ **在庫品緊急出荷の準備開始**
C⑫ **生産管理システムの応急復旧手段の検討**
C⑬ **生産管理部門は、サンプリングした生産装置台数を優先確認**
C⑭ **保守業者及び機器ベンダは特別体制**
C⑮ **関係省庁等への連絡、プレス対応**

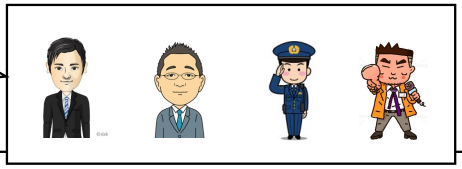
応急復旧を試み、生産継続する！

発注元在庫の2週間以内に応急復旧すれば影響はない！

ステージ④（省略）事態収束、原因調査、再発防止策検討段階

C⑯ 増産体制による**生産計画へのリカバー**

渉外戦略をどうする？



ステージ① 演習課題；
1．攻撃モデルAで製造装置（ライン）からのサイバー攻撃時、生産管理系や情報管理系に影響がある場合の対応はどのようになるか？
→対応規模が大きく拡大する
2．サイバー攻撃が引金事象である機器障害の場合、緊急事態対応計画での初動対処判断は通常の「主要設備故障、災害、商用電力中断時等」と何が違うか？
3．御社の工場で同種の初期症状があった場合、脅迫型ウイルスの侵入があったと気がつくか？
また、直ちに生産管理ネットワークの外部接続切断の発想は出てくるか？

本TTXは「研究型演習方式（全員参加型）」で実施します。
演習課題に対し、参加者全員で討議を行います。
自由に意見を述べ合ってください。
ファシリテータが追加解説を加えながら意見集約を行います。

まとめ

- 組織におけるミッション
- 組織のミッション継続をさまたげる要因
- サプライチェーンに対する攻撃
- 体験型演習のイメージの共有
- 中小製造業向け体験型演習シナリオのイメージの共有