サイバー演習の有効性
レジリエントな組織づくりに向けて

国立大学法人名古屋工業大学
青山 友美

Nagoya Institute of Technology

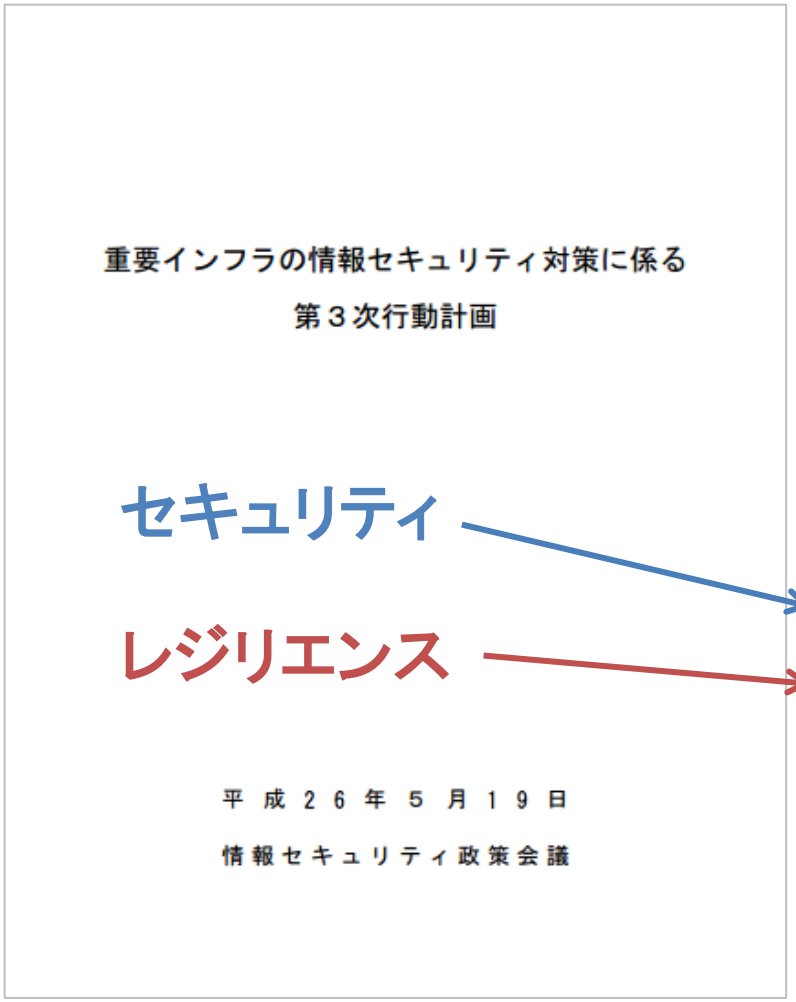
自己紹介

- 青山友美
- 名古屋工業大学大学院博士前期課程2年
- TUV SUD GmbH (ドイツ)インターンシップ
  - 8ヶ月
  - 消費者製品向け機能安全標準に関わる業務
- ENCS European Network for Cyber Security (オランダ)インターンシップ
  - 6ヶ月
  - 重要インフラむけセキュリティ演習のファシリテーションに参加

当セッションの目的

- ICS セキュリティに関連する演習の紹介
- レジリエンスの視点からの演習の比較
- 演習に何を効果として求めるべきか？
- 演習の成果をどのように持ち帰るべきか？

演習から何を学ぶ？



セキュリティ

レジリエンス

「重要インフラ防護」の目的

重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、IT障害の発生を可能な限り減らすとともにIT障害発生時の迅速な復旧を図ることで重要インフラを防護する。

NISC 重要インフラの情報セキュリティ対策に係る第3次行動計画(2014)
http://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf

演習から何を学ぶ？

the WHITE HOUSE PRESIDENT BARACK OBAMA

BRIEFING ROOM | ISSUES | THE ADMINISTRATION | PARTICIPATE | 1600 P

Home • Briefing Room • Statements & Releases

The White House

Office of the Press Secretary

E-Mail Tweet Share +

For Immediate Release February 12, 2013

Presidential Policy Directive -- Critical Infrastructure Security and Resilience

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

Introduction

The Nation's critica
coordinated efforts
– including assets,
and well-being.

大統領決定(PDD)21号(2013):重要インフラのセキュリティとレジリエンス（柔軟性）強化に向けた作業項目の策定

Presidential Policy Directive – PPD 21 (2013)
http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

セキュリティとレジリエンス

The terms "secure" and "security" refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

セキュリティとは、侵入・攻撃または天災・人災の結果に対する物理的手段または防衛サイバー対策によって、重要インフラへのリスクを低減すること。

The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

レジリエンス（柔軟性）とは、状況の変化に備え、適応し、混乱に耐えて急速に回復する能力を意味する。レジリエンスには意図的な攻撃、事故、及び 自然発生的な脅威またはインシデントに耐え、回復する能力が含まれる 。

Presidential Policy Directive – PPD 21 (2013)
http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

つまり？

- セキュリティ
  インシデントの発生するリスクを減らす
  ＝強い城壁を作りましょう
- レジリエンス
  インシデントに対応する力
  ＝強い組織を作りましょう

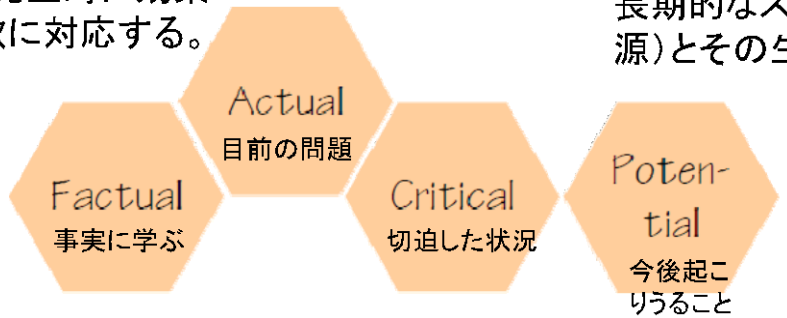
今回は、レジリエンスの観点から各演習に期待される学習効果を検証する

レジリエンスをつくるには

レジリエンス・エンジニアリングの考え方 (Resilience Engineering)

通常の、また通常以外の状況変化発生時に効果的かつ柔軟に対応する。

長期的なスレット（潜在的危害発生源）とその生起機会を予測する



過去の事象から、何が起きて何が原因だったのかを、正しく学ぶ。

短期的な展開とスレットを監視する。リスクモデルを更新する。

レジリエンス　4つの要因

対処能力 Respond	• 混乱・外乱にどのように対処すべきかを知っている
監視能力 Monitor	• 直近の脅威・またはそれになり得るものをどのように監視すべきか知っている
予見能力 Anticipate	• 未来に生じる変化・混乱・圧力およびその結果もたらされる事象の進展・脅威をどのように予見するべきか知っている
学習能力 Learn	• 成功・失敗事例からどのように教訓を得るのかを知っている

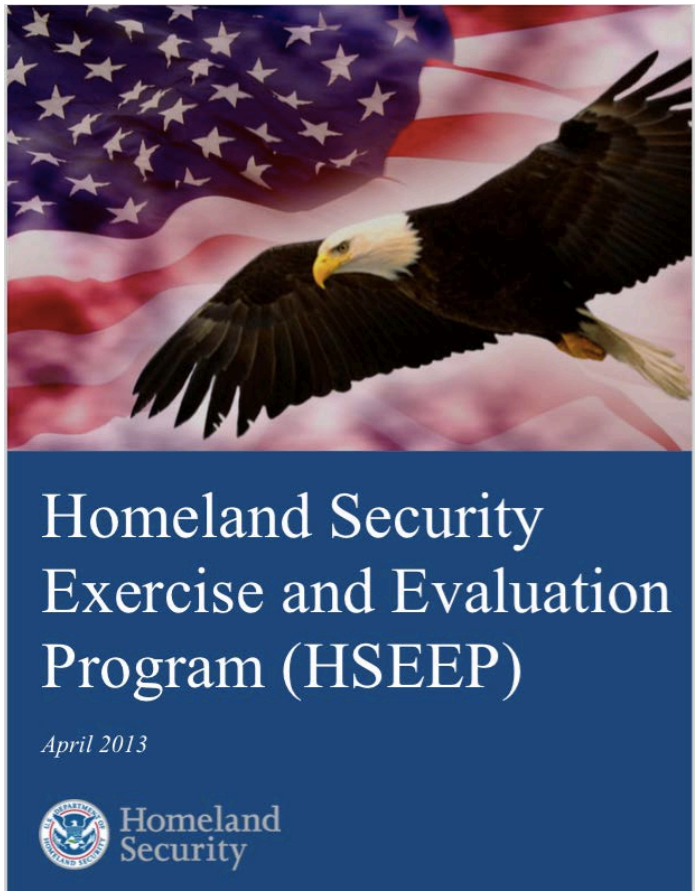
演習から学べるレジリエンス

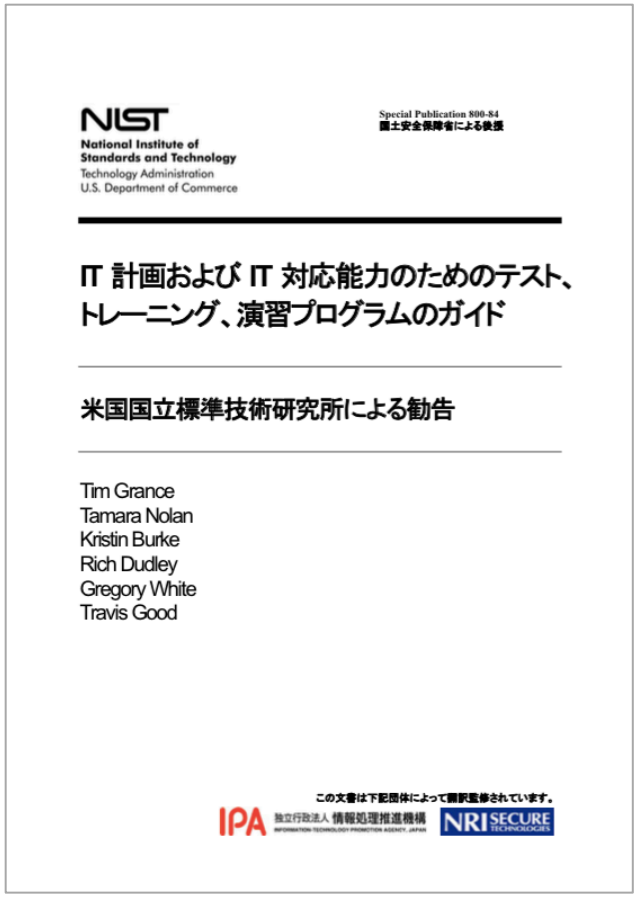
対処能力 Respond	• 混乱・外乱にどのように対処すべきかを知っている	インシデント対応手順
監視能力 Monitor	• 直近の脅威・またはそれになり得るものをどのように監視すべきか知っている	異常検知
予見能力 Anticipate	• 未来に生じる変化・混乱・圧力およびその結果もたらされる事象の進展・脅威をどのように予見するべきか知っている	セキュリティ脅威に関する知見
学習能力 Learn	• 成功・失敗事例からどのように教訓を得るのかを知っている	振り返り学習

今回比較する演習

- Red team – Blue team型演習（国外）
  - Idaho National Lab（米）/ ENCS（蘭）/ QUT （豪）
- ガス分野サイバーセキュリティ演習
  - CSSC 制御システムセキュリティセンター主催
- 分野横断的演習
  - NISC 内閣サイバーセキュリティセンター主催
- Cyber Range：APT（標的型攻撃）対応演習
  - JPCERT/CC 主催
- KIPS Kaspersky Industrial Protection Simulation
  - Kaspersky 主催

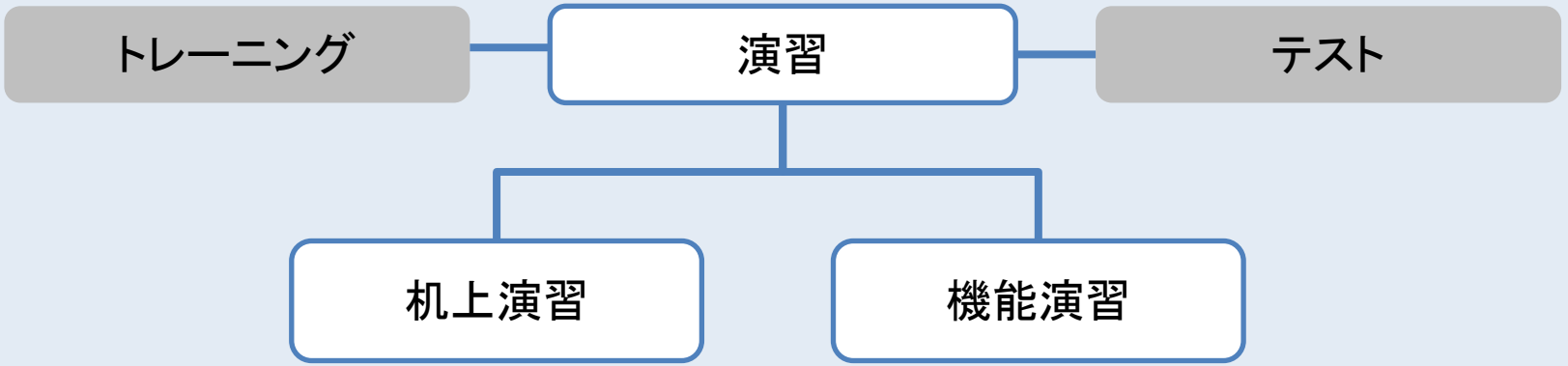
演習の種類





https://www.fema.gov/media-library/assets/documents/32326
https://www.ipa.go.jp/files/000025350.pdf

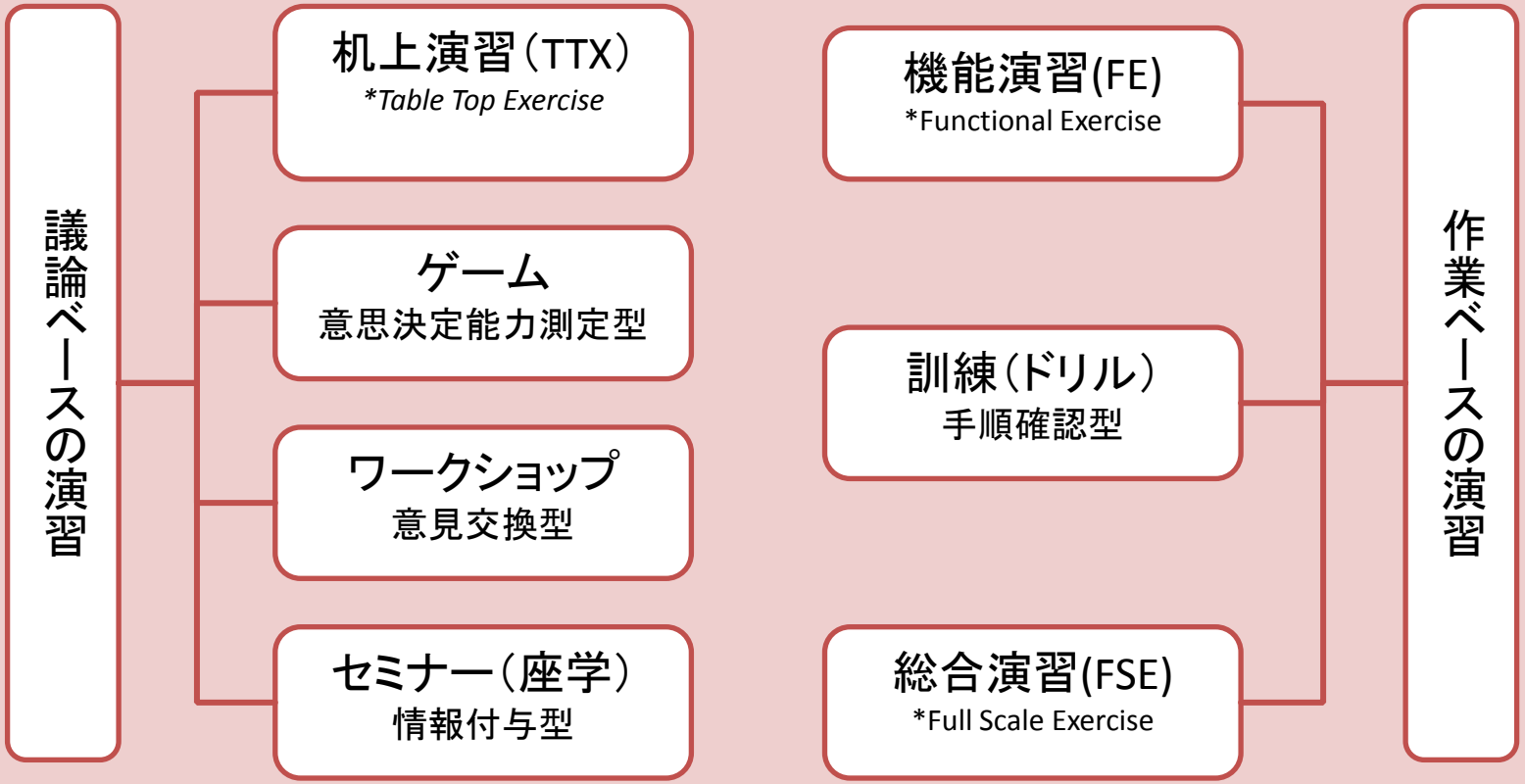
NIST Special Publication 800-84 による演習区分



- 緊急時対応計画やコンピュータセキュリティインシデント対応計画などのIT計画を実行する上で、例えば、計画における役割と責任を果たせるよう担当者の**トレーニング**を 行ったり、内容を検証するために計画の実施**演習**を行ったり、計画に指定されている運用環境でシステムとシステム構成要素の運用性を確認する**テスト**を実施する、といった準備(**TT&E/Test, Training and Exercise**)がなされているべきてある。
- **机上演習**は、議論ベースの演習で、緊急時の役割や、ある特定の緊急事態への対応策を議論する形をとる。
- **機能演習**を実施することで、スタッフは実際の緊急事態における役割と責任を、シミュレ ーション環境のなかで実践することが可能となる。

NIST SP 800-84 “IT 計画および IT 能力のためのテスト、トレーニング、演習プログラムのガイド” ` https://www.ipa.go.jp/files/000025350.pdf

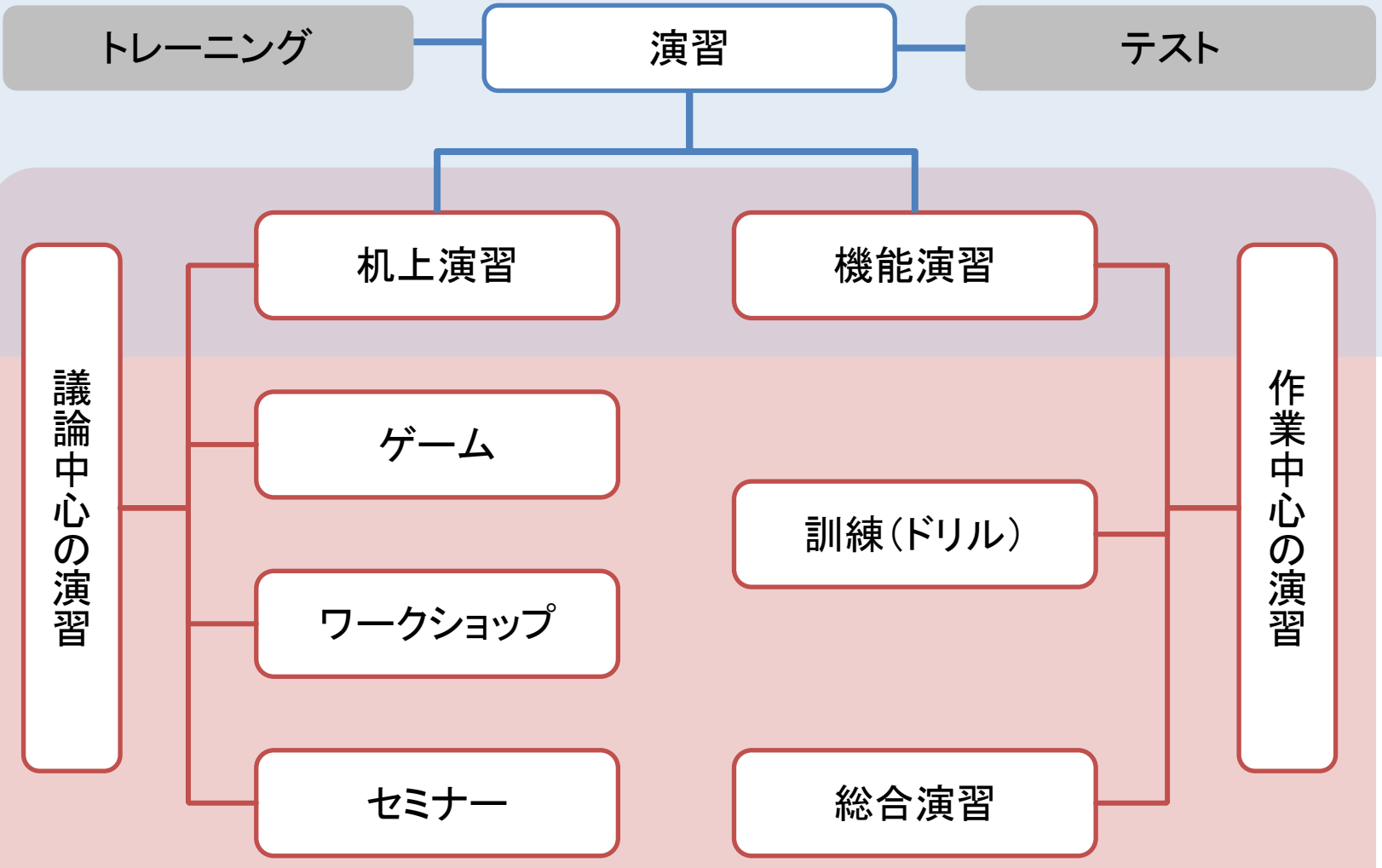
HSEEP(Homeland Security Exercise and Evaluation Program) による演習区分



- 議論ベースの演習では、ファシリテーターおよびプレゼンターが議論の進行を務め、参加者が演習の目的に向かって議論を進めるよう働きかける。
- 作業ベースの演習において、参加者は演習のシナリオに対し情報伝達や人的資源管理など、実際の行動によって反応する。

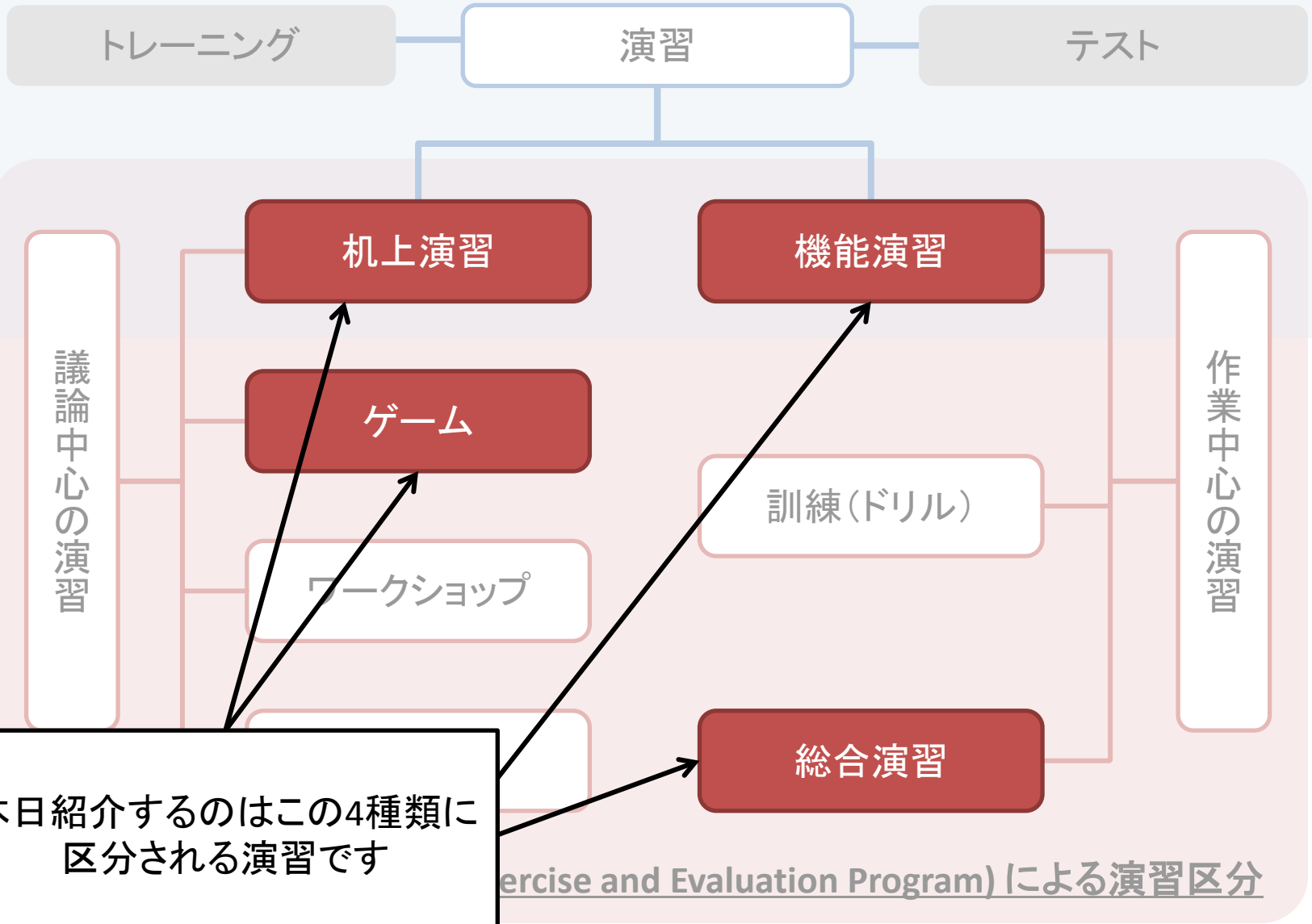
Homeland Security Exercise and Evaluation Program
https://www.fema.gov/media-library/assets/documents/32326

NIST Special Publication 800-84 による演習区分



HSEEP(Homeland Security Exercise and Evaluation Program) による演習区分

NIST Special Publication 800-84 による演習区分



ercise and Evaluation Program) による演習区分

演習の比較

- **Red team – Blue team型演習（国外）**
  - **Idaho National Lab（米）/ ENCS（蘭）/ QUT （豪）**
- ガス分野サイバーセキュリティ演習
  - CSSC 制御システムセキュリティセンター主催
- 分野横断的演習
  - NISC 内閣サイバーセキュリティセンター主催
- Cyber Range：APT（標的型攻撃）対応演習
  - JPCERT/CC 主催
- KIPS Kaspersky Industrial Protection Simulation
  - Kaspersky 主催

INL アイダホ国立研究所

Source: https://secure.inl.gov/icsadv1214/

ENCS – European Network for Cyber Security

The ENCS Advanced Cyber Security Course
5 Days of learning about cyber security from both sides

Days 1 – 3: Basic knowledge and skills

In the first three days experts from ENCS and its international network of partners will teach you the basic knowledge and skills you need. You will apply what you learn immediately in hands-on sessions.

Offense:
Learn how hackers operate.
- How they scan your network to prepare for attacks.
- How they exploit vulnerabilities in software to hack a computer (Wurldtech).
- How they crack weak passwords.
- How they extract confidential information from websites.

Defense:
Learn what you can do to stop them.
- Find vulnerabilities before hackers do.
- Detect intrusions in your network (SourceFire).
- Collect evidence of an incident (Netherlands Forensic Institute).
- Know which security standards apply to your organization.

Day 4: Red Team - Blue Team exercise

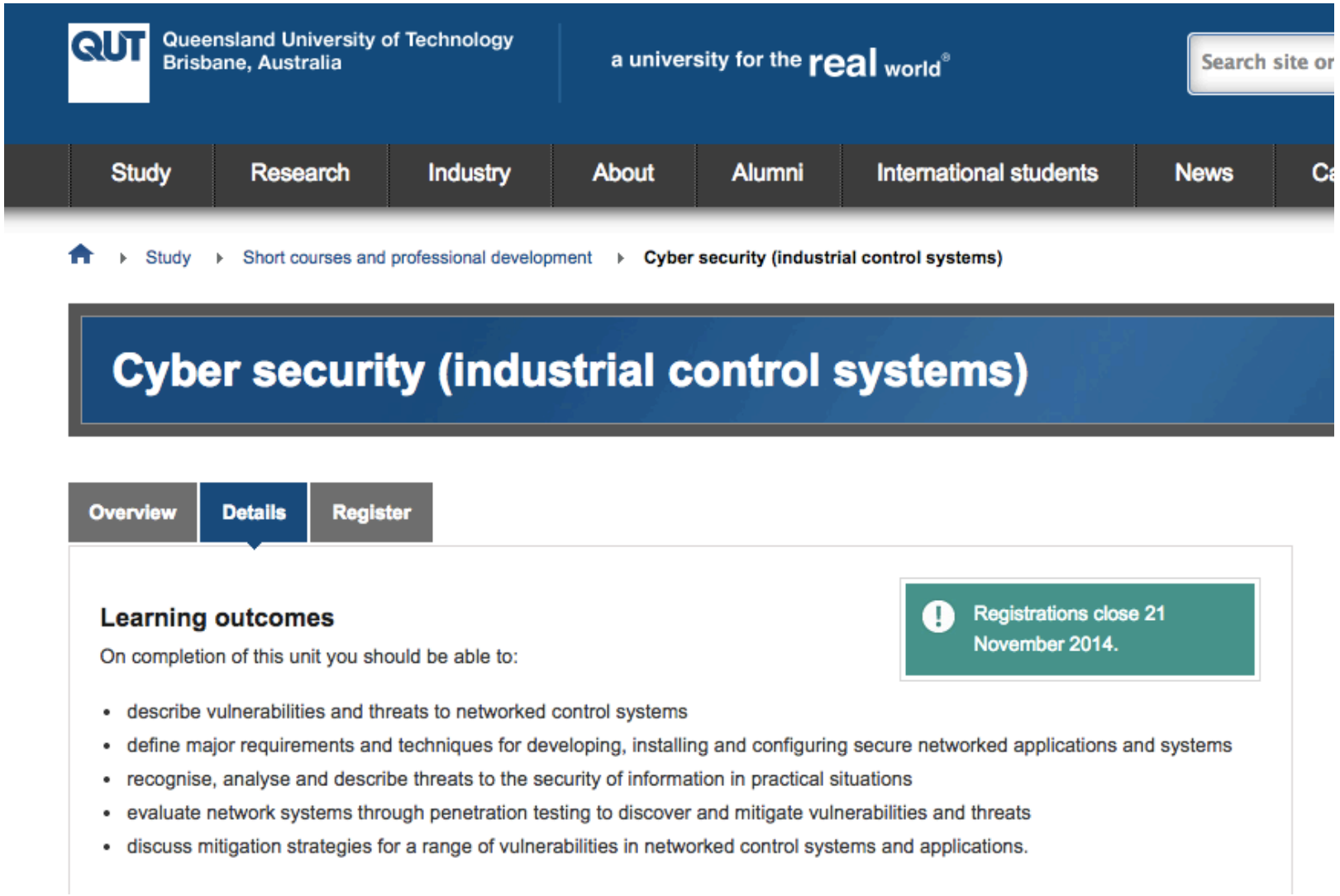
In this realistic cyber attack-and-defense exercise, you are challenged to apply all your intelligence and the knowledge you've gained. ENCS offers a real-life business environment, including an operational ICS environment controlling a small factory. It is the Blue Team's responsibility to secure the factory and keep production going, while at the same time the Red Team is hacking their systems.

Day 5: Evaluation and lessons learned

On the final course day you will discuss the exercise. What did the people in the other team, or those in different roles, experience? How can you apply the lessons learned within your own company? The objective is that you will take home concrete, practical steps to improve the cyber security of your own organization.

Source: https://education.encs.eu/training/training-overview/encs-advanced-cyber-security-course-red-team-blue-team-training

QUT クイーンズランド工科大学



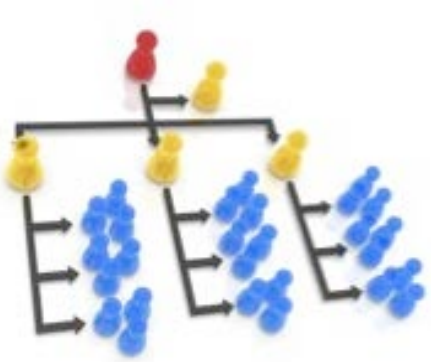
Source: https://www.qut.edu.au/study/short-courses-and-professional-development/short-courses/cyber-security-industrial-control-systems

ENCS / INL / QUT
Red team – Blue team型演習

主催者	INL (Idaho National Lab.) アイダホ国立研究所	ENCS (European Network for Cyber Security)	QUT (Queensland University of Tech.) クイーンズランド工科大学
開催地 国・都市	米国・アイダホ州	オランダ・ハーグ	オーストラリア・ ブリスベン
主催機関	ICS-CERT	研究機関	大学
講師	専属講師・研究者	研究者+招待講演者 （ベンダー・セキュリティ企業等）	教授(ITセキュリティ)
開催頻度	2ヶ月に1度	半年に1度	年に1度

ENCS / INL / QUT
Red team – Blue team型演習

Blue Team



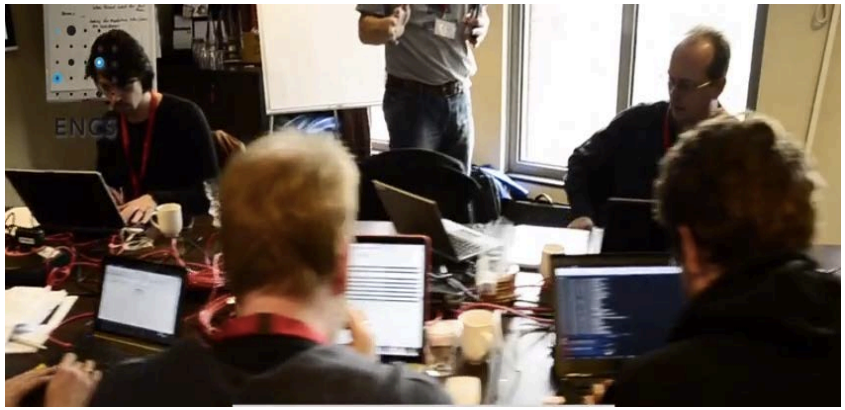
- 防御チーム
- 20名程度
- シナリオ
  - 化学製品を生産するプラント
  - 参加者がそれぞれマネージャー・IT管理者・オペレータなどの役職を演じる

Red Team

- 攻撃チーム
- 10名程度
- シナリオ
  - ブルーチームの敵対企業に雇われたハッカー集団
  - 生産の妨害・システムの破壊が最終目的

ENCS / INL / QUT
Red team – Blue team型演習

日程	3 – 5 日
コース構成	座学＋作業演習
参加者数	20 - 30 名
参加対象者	IT/制御/マネジメント
演習タイプ	総合演習・敵対型
演習環境	フルスケール
シナリオ	仮想企業
アクティビティ	参加者の自由
長所	フルスケールに再現されたネットワーク構成での実戦
短所	参加者によって学習効果にばらつき



ENCS 演習紹介ビデオより
http://youtu.be/BGVwOJw1DfY

ENCS / INL / QUT
Red team – Blue team型演習

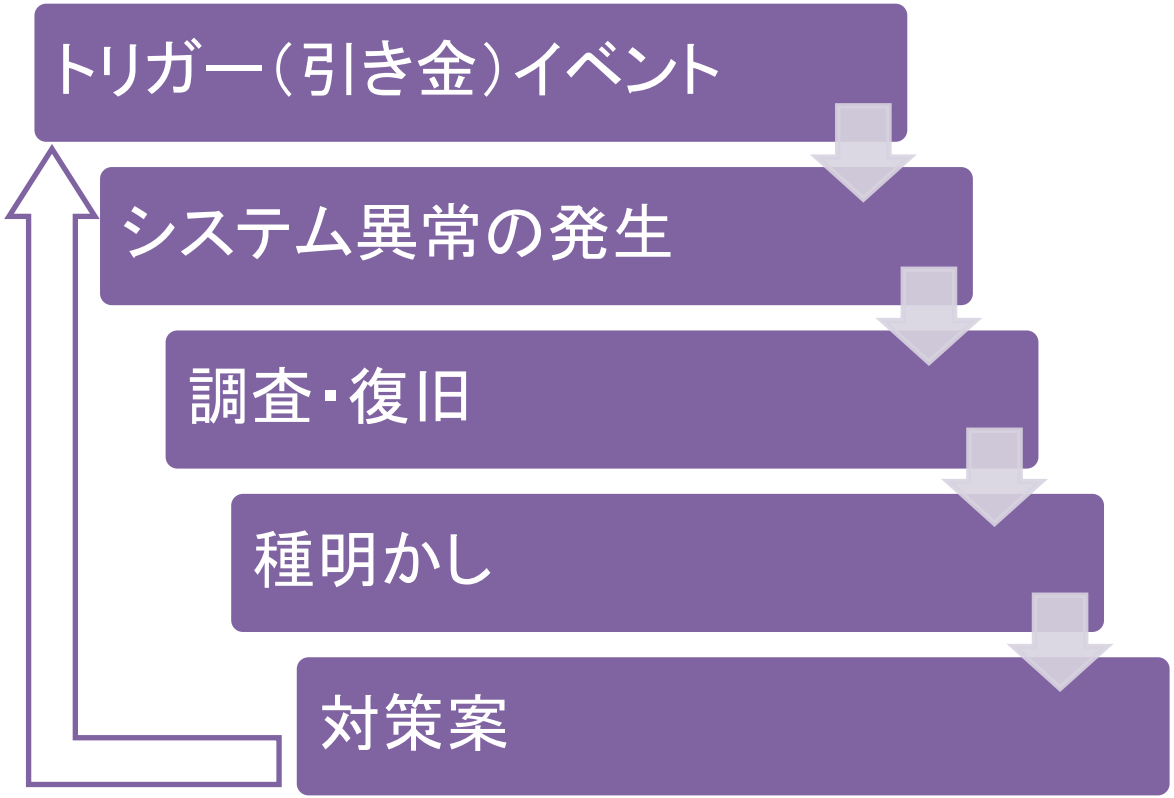
インシデント対応手順	• 意思決定層の対応手順・IT技術の対応手順を仮想企業において体験 • インシデント対応におけるコミュニケーション
異常検知	• IT技術による異常検知手法 • 攻撃者の視点でネットワークの脆弱性を探す視点
セキュリティ脅威に関する知見	• 攻撃視点・防御視点の両方からインシデントを経験 • インシデント発生によって社内に起こり得るトレードオフ（セキュリティvs生産性、効率vs完璧さ）を体験

演習の比較

- Red team – Blue team型演習（国外）
  - Idaho National Lab（米）/ ENCS（蘭）/ QUT （豪）
- **ガス分野サイバーセキュリティ演習**
  - **CSSC 制御システムセキュリティセンター主催**
- 分野横断的演習
  - NISC 内閣サイバーセキュリティセンター主催
- Cyber Range：APT（標的型攻撃）対応演習
  - JPCERT/CC 主催
- KIPS Kaspersky Industrial Protection Simulation
  - Kaspersky 主催

サイバーセキュリティ演習
CSSC 制御システムセキュリティセンター

演習の構成



写真：2013年度に実施したサイバーセキュリティ演習の概要説明資料より
http://www.css-center.or.jp/pdf/cybersecurity-exercises_outline.pdf

サイバーセキュリティ演習
CSSC 制御システムセキュリティセンター

日程	2 日
コース構成	座学＋機能演習
参加者数	20 - 30 名
参加対象者	ガス・化学・ビル・電気事業者
演習タイプ	防御デモを5シナリオ
演習環境	実機（オペレーション部分のみ）
シナリオ	仮想ガスプラント会社
アクティビティ	段階的に指示
長所	オペレーション機能に集中した演習 演習後、各社毎に有識者との個別議論有り
短所	参加対象分野に制限

CSSC 演習紹介ビデオより
http://youtu.be/aqRB7wfR4AQ

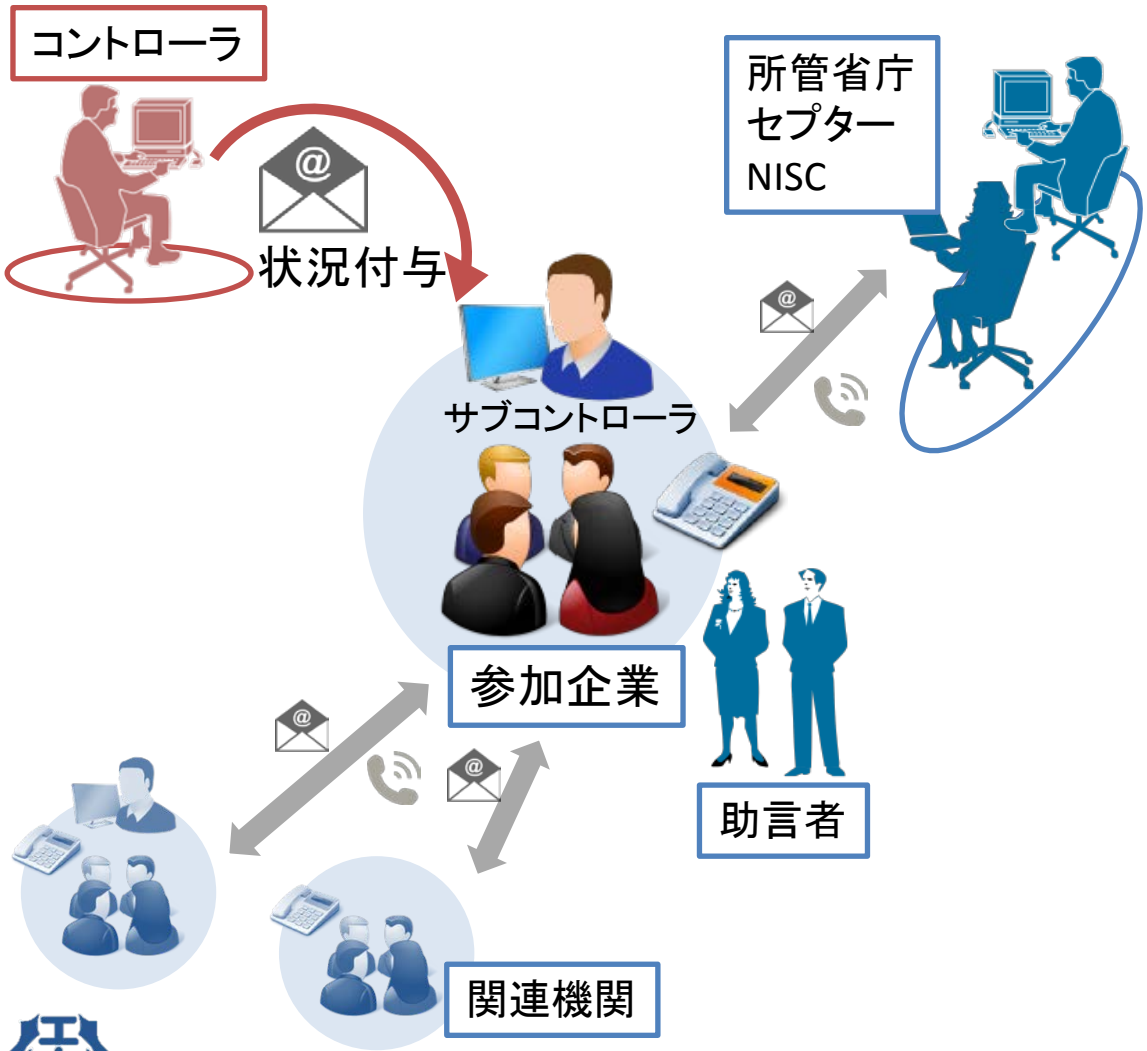
サイバーセキュリティ演習
CSSC 制御システムセキュリティセンター

インシデント対応手順	• オペレータ層のインシデント対応手順をデモプラントで体験
異常検知	• オペレータによる異常の検知方法 • セキュリティインシデントとセーフティインシデントの見え方の違い
セキュリティ脅威に関する知見	• 攻撃の侵入経路 • 攻撃のバリエーション • 効果的な対策手法

演習の比較

- Red team – Blue team型演習（国外）
  - Idaho National Lab（米）/ ENCS（蘭）/ QUT （豪）
- ガス分野サイバーセキュリティ演習
  - CSSC 制御システムセキュリティセンター主催
- **分野横断的演習**
  - **NISC 内閣サイバーセキュリティセンター主催**
- Cyber Range：APT（標的型攻撃）対応演習
  - JPCERT/CC 主催
- KIPS Kaspersky Industrial Protection Simulation
  - Kaspersky 主催

分野横断的演習
NISC 内閣サイバーセキュリティセンター主催



全体会合

機能演習

写真：2014年演習より

分野横断的演習
NISC 内閣サイバーセキュリティセンター主催

日程	1日
コース構成	機能演習
参加者数	348名 （94組織）
参加対象者	重要インフラ13分野
演習タイプ	防御2シナリオ
演習環境	連絡ツールのみ実機
シナリオ	自社・自役職
アクティビティ	参加者の自由
長所	分野横断した情報共有練習 サブ・コントローラによるシナリオ調整
短所	達成目標・シナリオの再現度の設定は参加者次第

Twitter @cas_nisc
内閣サイバーセキュリティセンター公式アカウントより

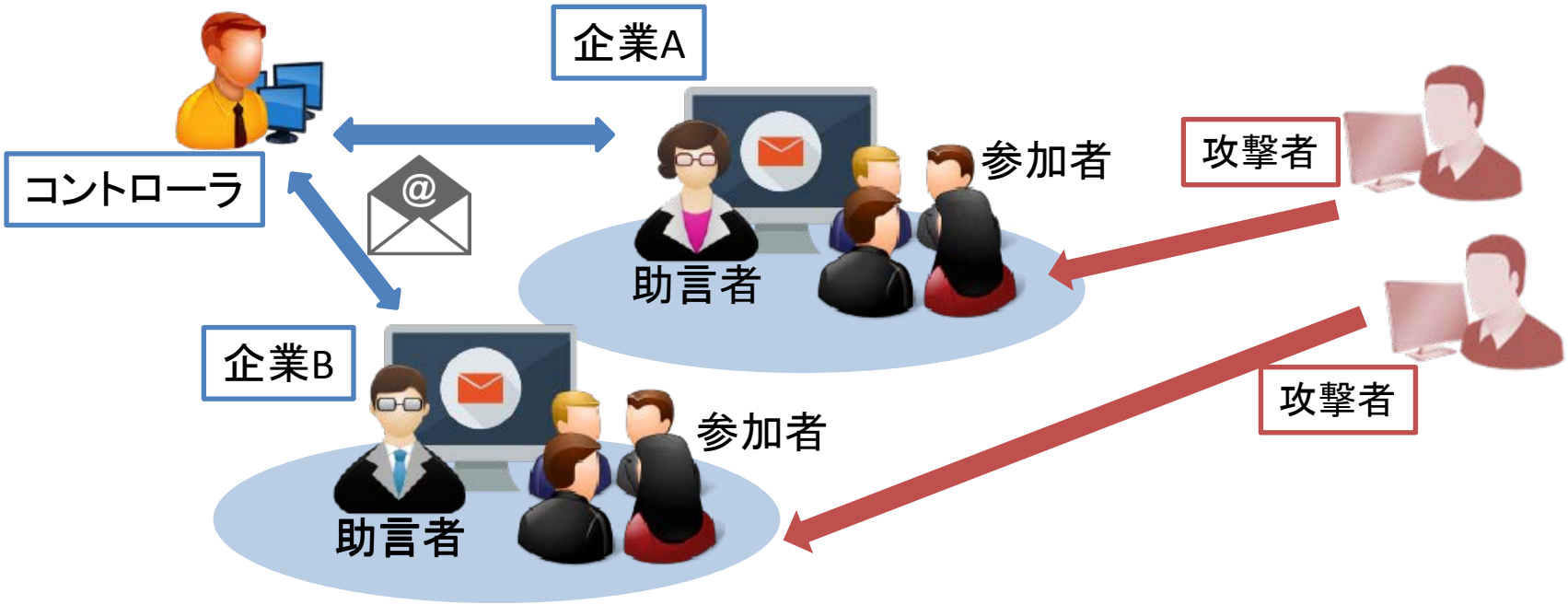
分野横断的演習
NISC 内閣サイバーセキュリティセンター主催

インシデント対応手順	• 自社で取り決められている意思決定層の対応手順 • 情報共有体制の実効性を検証 • 事業継続計画の発動方法や、その手順を確認
異常検知	• （参加者側からアクティブに異常検知をして発信することはない）
セキュリティ脅威に関する知見	• 状況が次第に明らかになっていく過程で、システムへの影響や被害の及ぶ範囲を想像する

演習の比較

- Red team – Blue team型演習（国外）
  - Idaho National Lab（米）/ ENCS（蘭）/ QUT （豪）
- ガス分野サイバーセキュリティ演習
  - CSSC 制御システムセキュリティセンター主催
- 分野横断的演習
  - NISC 内閣サイバーセキュリティセンター主催
- **Cyber Range：APT（標的型攻撃）対応演習**
  - **JPCERT/CC 主催**
- KIPS Kaspersky Industrial Protection Simulation
  - Kaspersky 主催

Cyber Range：APT（標的型攻撃）対応演習
JPCERT/CC



参加者は攻撃に対する技術対応に加えて、
コントローラの指示によって議論も行う

Cyber Range：APT（標的型攻撃）対応演習
JPCERT/CC

日程	1日
コース構成	機能演習と机上演習の組み合わせ
参加者数	最大2グループ、10名程度
参加対象者	IT 管理者
演習タイプ	防御チーム
演習環境	IT部分実機
シナリオ	仮想企業
アクティビティ	段階的に指示
長所	チームごとに助言者がつき、議論をサポート インシデント対応の手順を段階的に体験
短所	IT管理者に限定・制御システム系のインシデントでない

Cyber Range：APT（標的型攻撃）対応演習
JPCERT/CC

インシデント対応手順	• IT管理者の技術的対応手順を、指示を受けながら学ぶ • 関連機関との情報共有の重要性を学ぶ
異常検知	• （参加者側からアクティブに異常検知をして発信することはない）
セキュリティ脅威に関する知見	• APT(標的型攻撃)の攻撃手法を体験する • 攻撃トレンド情報などから、自社で起きているインシデントの全体図を想像する

演習の比較

- Red team – Blue team型演習（国外）
  - Idaho National Lab（米）/ ENCS（蘭）/ QUT （豪）
- ガス分野サイバーセキュリティ演習
  - CSSC 制御システムセキュリティセンター主催
- 分野横断的演習
  - NISC 内閣サイバーセキュリティセンター主催
- Cyber Range：APT（標的型攻撃）対応演習
  - JPCERT/CC 主催
- **KIPS Kaspersky Industrial Protection Simulation**
  - **Kaspersky 主催**

Kaspersky Lab

KIPS “Kaspersky Industrial Protection Simulation”

目標：企業のITスペシャリストとして、セキュリティを強化しながら売り上げを伸ばす

メッセージフェーズ

- 業界ニュース・社内メッセージなど
- 対策が必要かどうか各チームで判断

アクションフェーズ

- チームで話し合い、選択するカードを決定する

生産フェーズ

- シナリオに沿って選択したカードの効果・影響が売り上げ高・攻撃の進捗度に表れる

全部で5ターン繰り返す

Kaspersky Lab

KIPS “Kaspersky Industrial Protection Simulation”

日程	2 時間程度
コース構成	ゲーム
参加者	12名（4チーム）より
参加対象者	誰でも可能
演習タイプ	防御シナリオ
演習環境	ボード・カードゲーム
シナリオ	仮想企業
アクティビティ	カードから選択
長所	簡単にサイバー攻撃を体験 スコア($)によるわかりやすいフィードバック
短所	対策の選択はカードからの選択に限られる

KIPS紹介ビデオより
http://www.kaspersky.com/industrial-security-cip

Kaspersky Lab

KIPS “Kaspersky Industrial Protection Simulation”

インシデント対応手順	• カードから選んだ対策の効果が次のターンでシステムへ反映される
異常検知	• 「業界ニュース」などとして入って来る情報からサイバー攻撃の可能性を想像する • 「システム監査」カード導入のタイミング
セキュリティ脅威に関する知見	• セキュリティ対策の導入と生産のバランスを考える

まとめ

- 演習によって**学べる知識・スキルは異なる**
  - 攻撃手法・インシデントハンドリング手順…
- 演習内で**行う活動・意思決定も異なる**
  - IT/オペレータ技術対応・事業継続計画・議論

…「この演習を受けておけば対策は完璧」ということはない

総括

	ENCS / INL / QUT	CSSC	NISC	JPCERT/CC	Kaspersky Lab
インシデント対応手順	意思決定層の対応手順・IT技術の対応手順を仮想企業において体験	オペレータ層のインシデント対応手順をデモプラントで体験	自社で取り決められている意思決定層の対応手順	IT管理者の技術的対応手順を、指示を受けながら学ぶ	カードから選んだ対策の効果が次のターンでシステムへ反映される
	インシデント対応におけるコミュニケーション		情報共有体制の実効性を検証	関連機関との情報共有の重要性を学ぶ	
			事業継続計画の発動方法や、その手順を確認		
異常検知	IT技術による異常検知手法	オペレータによる異常の検知方法	（参加者側からアクティブに異常検知をして発信することはない）	（参加者側からアクティブに異常検知をして発信することはない）	「業界ニュース」などとして入って来る情報からサイバー攻撃の可能性を想像する
	攻撃者の視点でネットワークの脆弱性を探す視点	セキュリティインシデントとセーフティインシデントの見え方の違い			「システム監査」カード導入のタイミング
セキュリティ脅威に関する知見	攻撃視点・防御視点の両方からインシデントを経験	攻撃の侵入経路	状況が次第に明らかになっていく過程で、システムへの影響や被害の及ぶ範囲を想像する	APT(標的型攻撃)の攻撃手法を体験する	セキュリティ対策の導入と生産のバランスを考える
	インシデント発生によって社内に起こり得るトレードオフを体験	攻撃のバリエーション		攻撃トレンド情報などから、自社で起きているインシデントの全体図を想像する	
		効果的な対策手法			

演習はPDCAサイクルのドライバー

- 「課題を抽出する場」
  - CSSC 制御システムセキュリティセンター
- 「気づきを得る場」
  - NISC 内閣サイバーセキュリティセンター

- 演習成果を自社に持ち帰る
- 自社の体制を自己評価する

実はもう一つ…
演習から学べるレジリエンス

対処能力 Respond	• 混乱・外乱にどのように対処すべきかを知っている	インシデント対応手順
監視能力 Monitor	• 直近の脅威・またはそれになり得るものをどのように監視すべきか知っている	異常検知
予見能力 Anticipate	• 未来に生じる変化・混乱・圧力およびその結果もたらされる事象の進展・脅威をどのように予見するべきか知っている	セキュリティ脅威に関する知見
学習能力 Learn	• 成功・失敗事例からどのように教訓を得るのかを知っている	**振り返り**

「振り返りの時間」の重要性

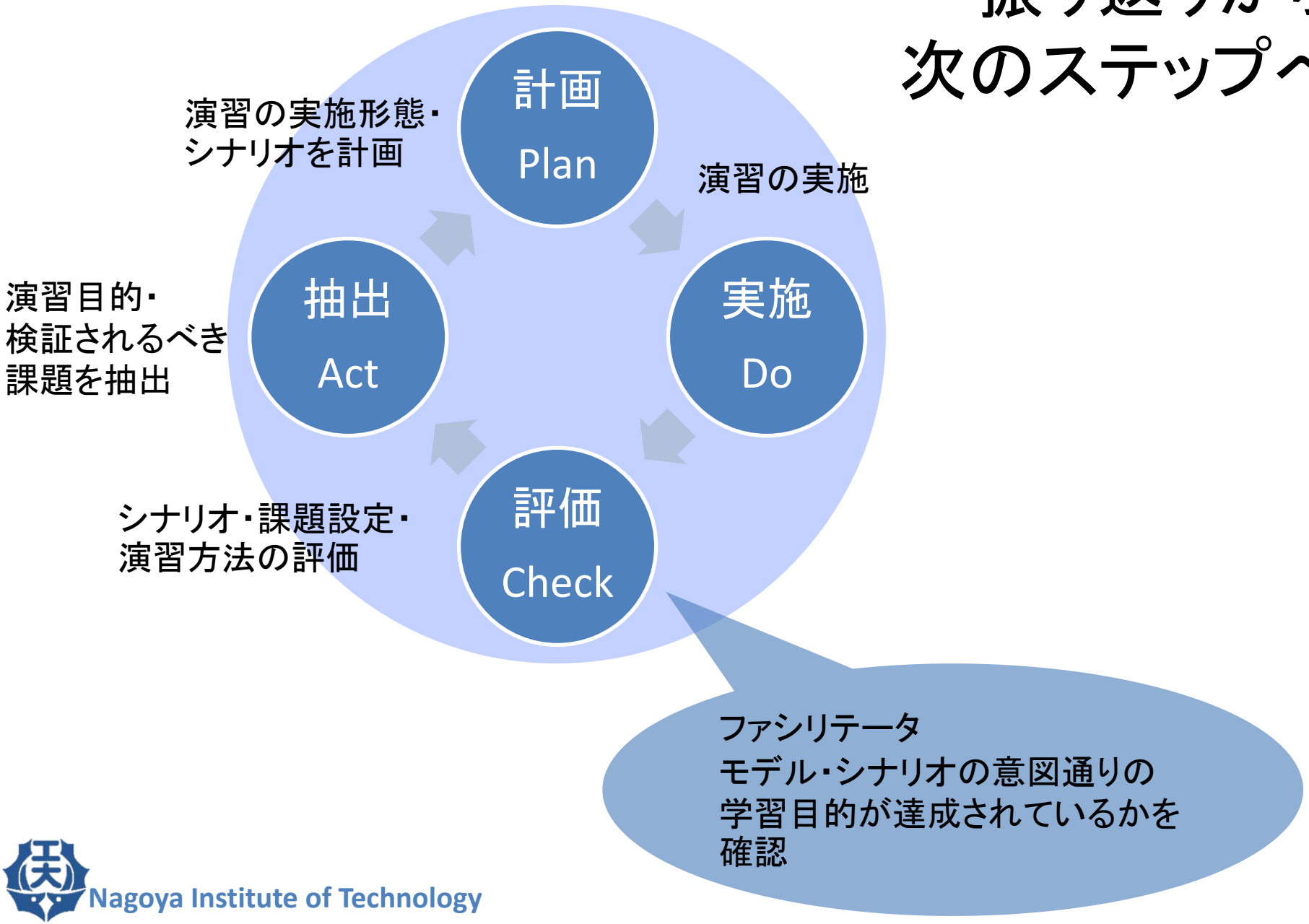
- どの演習においても、演習終了後にファシリテータ・参加者全員で演習の「振り返り」（デブリーフィング）を行う
- 「振り返り」は答え合わせではなく演習での体験を知識に落とし込む作業

ファシリテータ
モデル・シナリオの意図通りの学習目的が達成されているかを確認

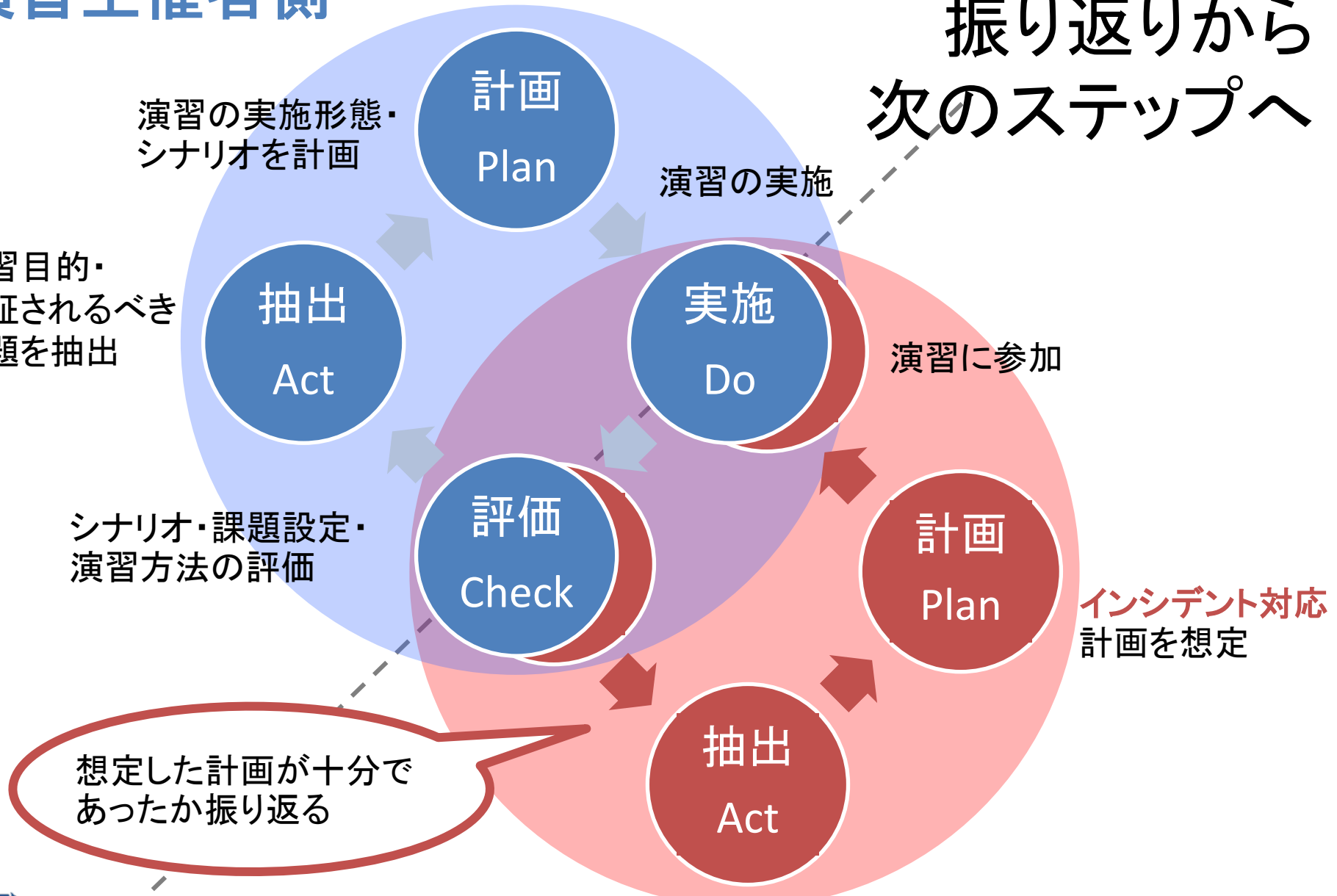
参加者
体験した事象（主観的な経験）をシェアする・他の参加者の体験を聞くことで共通の教訓を得る

演習主催者側

振り返りから次のステップへ



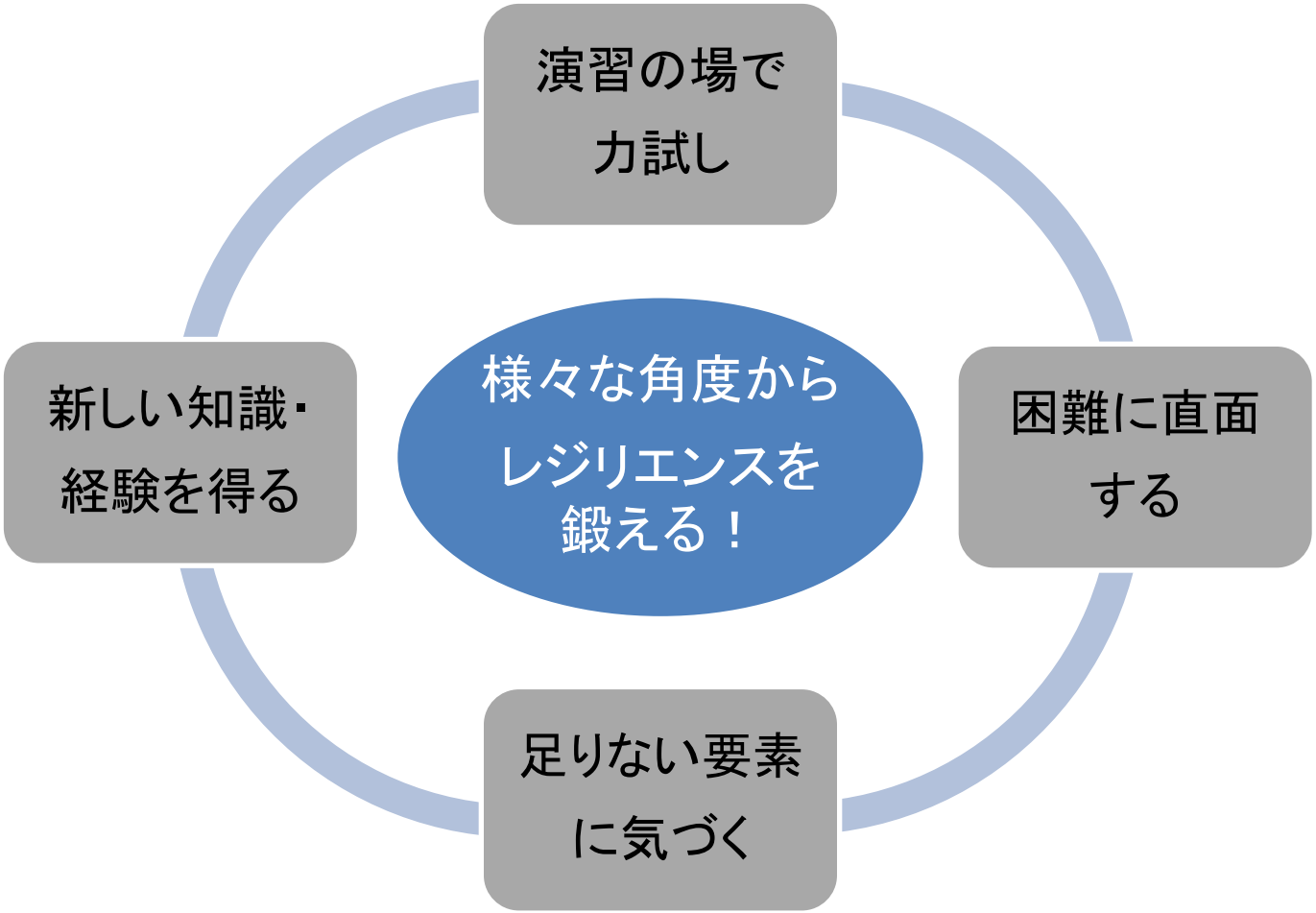
演習主催者側



振り返りから
次のステップへ

演習参加者側

演習の効果


演習の場で
力試し
困難に直面
する
足りない要素
に気づく
新しい知識・
経験を得る
様々な角度から
レジリエンスを
鍛える！

次世代型演習に向かって

- インシデント対応手順を自社のモノとする
  - 演習体験を参加者個人から組織へ展開
    - 体験を自社で適用する方策欠如の問題
  - 他組織との連携で、組織として対応を図る
    - 自社能力（インシデント対応、BCP）の客観的評価の問題
- 異常検知を網羅する
  - 異常検知能力の向上
    - 安全に関わるサイバーインシデントに気付く能力構築の問題
  - 異常検知範囲の拡大
    - 安全に関わるサイバーインシデントに気付くスタッフの教育問題
- セキュリティ脅威に関する知見の拡充
  - 攻撃者の視点（思考）を勘案した対抗処置
  - 攻撃者の心理（ストレス）を勘案した対抗処置
  - 攻撃者の技術を勘案した対抗処置

青山友美
t.aoyama.084@nitech.jp

ご静聴ありがとうございました