ロールプレイ型
サイバー攻撃演習/訓練
実施マニュアル

2023年3月20日

日本コンピュータセキュリティインシデント対応チーム協議会
インシデント対応訓練ワーキンググループ

目次

第1章
はじめに

本書の目的

■「サイバー攻撃演習/訓練実施マニュアル」では、以下の整理によりサイバー攻撃の演習/訓練のスムーズな運営を支援することを目的とする

■サイバー攻撃演習/訓練実施の実施手法を取りまとめる

⑩演習/訓練における実施事項をSTEPに分割し、各STEPで何をすべきかわかるようにする

■サイバー攻撃演習/訓練の全体像を示す

⑩どのようなタイプのサイバー攻撃演習/訓練を実施すればよいかを選択できるようにする

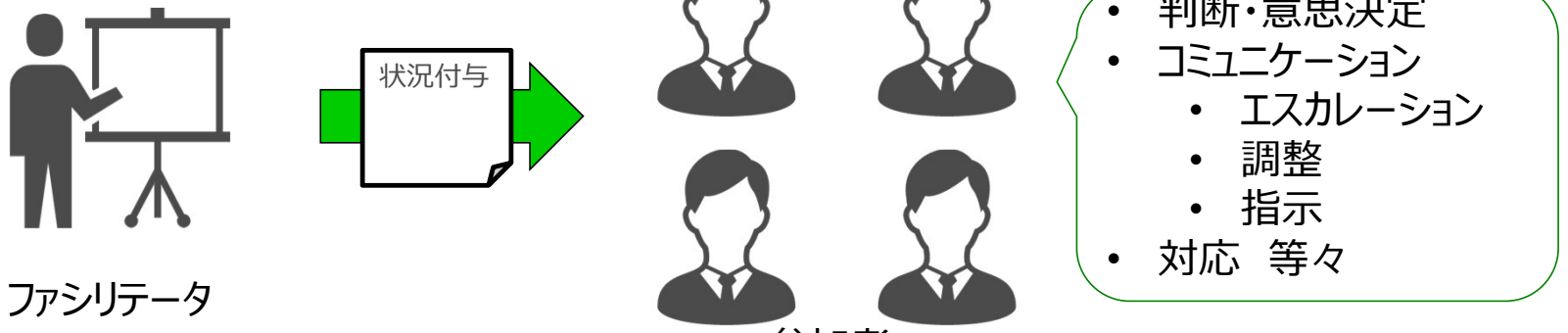
⑩演習/訓練を難易度で分類し、CSIRTの成熟度に沿ったロードマップ作成に関する指針として利用できるようにする

■本書では、ロールプレイ形式での演習/訓練に関して記述する

サイバー攻撃演習/訓練とは

- サイバー攻撃に関する状況付与により、発生しているインシデントへの対応検討を行う演習/訓練である
  - 参加者はインシデントが発生した際に、その対応として、関係者間でどのような対応を実施すべきかの検討や、検討事項が実施できるか等の確認を実施する
  - サイバー攻撃演習/訓練を通して気づいた点や反省点を振り返り、課題等の抽出を実施する

サイバー攻撃演習/訓練イメージ



サイバー攻撃演習/訓練の必要性

■サイバー攻撃への対応は様々な状況判断、対処や連携が必要

■サイバー攻撃演習/訓練を実施していないと、不測の事態が起こった際に、担当者が緊急時に適切に行動することが出来ない

インシデント対応力を発展させていくために、

継続的なサイバー攻撃演習/訓練の実施が必要

サイバー攻撃演習/訓練の必要性：フレームワーク

■サイバー攻撃演習/訓練に関して言及しているフレームワーク等を以下に例示する

■様々なフレームワークにより演習/訓練の必要性が言及されており、CSIRTは継続的な演習/訓練の実施が必要である

ドキュメント	概要
サイバーセキュリティ経営ガイドライン	大企業及び中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要１０項目」をまとめたものである。 ここでは、「指示７ インシデント発生時の緊急対応体制の整備」において、CSIRTの整備と演習の実施が言及されている。
FIRST CSIRT Services Framework	FIRSTの定義したCSIRTのサービスを定義したフレームワークである。ここでは、5つのサービスエリアが定義されており、そのうちの一つのサービスエリアである「知識移転」において、演習がCSIRTのサービスとして定義されている。
Cybersecurity Framework	NIST が政府や民間から意見を集め作成した、サイバーセキュリティ対策に関するフレームワーク。サブカテゴリ― PR-IP10では、「対応計画と復旧計画がテストされている」、サブカテゴリ―DE.DP-3では「検知プロセスがテストされている」と定義されている。

演習と訓練の差異（1/2）

■混合しがちな訓練と演習であるが、本書では以下のように定義する。

Q 22300：2013（ISO 22300：2012）での定義			特徴
日本語	英語	用語定義	
演習	exercise	組織内で、パフォーマンスに関する教育訓練を実施し、評価し、練習し、改善するプロセス 注記1 演習は、次のような目的のために利用することができる。 – 方針、計画、手順、教育訓練、装置又は組織間合意の妥当性確認 – 役割及び責任を担う要員の明確化並びにそれらの教育訓練 – 組織間の連携及びコミュニケーションの改善 – 資源の不足部分の特定 – 個人のパフォーマンスの改善、及び改善の機会の特定 – 臨機応変な対応を練習する統制された機会	大きな目的は「検証」となる 万が一、演習の途中で重大な問題が見つかって演習を中断せざるを得なくなったとしても、それは演習を行うことによって問題を発見できた結果として、演習としては成果があるものとしてみなされる
訓練	drill	ある特定の技能を練習し、複数回の繰返しを伴うことが多い活動	大きな目的は「技能の習得」である 訓練が途中で中断してしまった場合、目的とする特定の技能を習得できないこととなり、訓練は失敗となる 初歩的・基礎的なレベルから高度に複雑なレベルへ段階を踏むのが通常の方法である

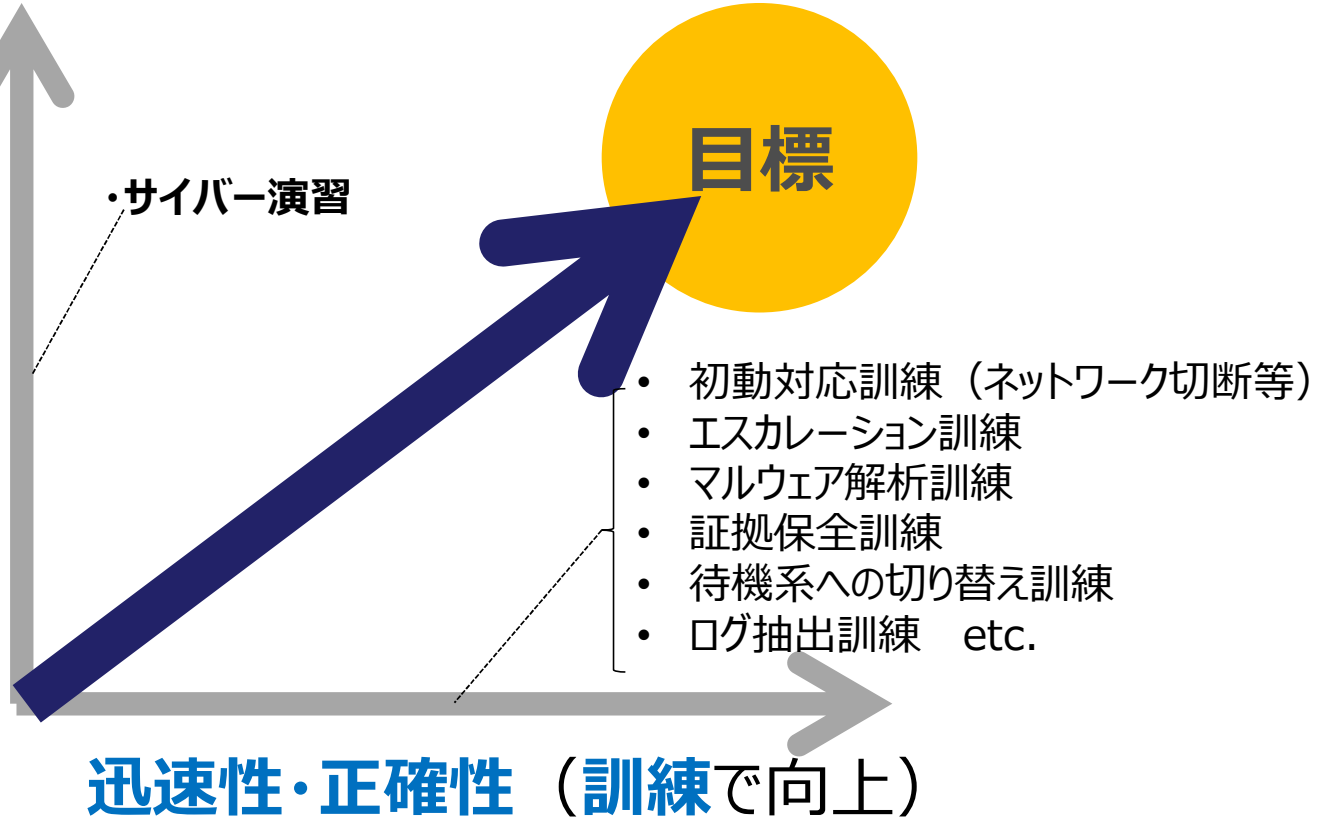
演習と訓練の差異（2/2）

■**訓練**と**演習**の両軸でインシデント対応能力を向上させる

サイバー・レジリエンス
（**演習**で向上）

“Cyber Resilience”
(**NIST SP800-160 Vol2 Rev.1**)
サイバー資源を保有するシステムが、困難な状況やストレスに置かれたり、攻撃、侵害を受けることを、予測し、耐え、回復し、適応する能力

※ **レジリエンス（resilience）**：
弾力、復元力、回復力
⇒困難な状況下に置かれても、柔軟に適用して生き延びる力



第2章
サイバー攻撃演習/訓練実施のためのSTEP

サイバー攻撃演習/訓練実施のためのSTEP

■サイバー攻撃演習/訓練は以下のSTEPで実施の検討を行う

■STEP1　：プロジェクトの構築
■STEP2　：情報収集
■STEP3　：計画の作成
■STEP4　：シナリオ検討
■STEP5　：実施準備・実施
■STEP6　：実施後対応

STEP1
プロジェクトの構築

STEP1
プロジェクトの構築

■CSIRTを中心にサイバー攻撃演習/訓練プロジェクトの構築を実施する

■実施するサイバー攻撃演習/訓練の目的により、プロジェクトメンバの構成は最適な体制が異なる場合もあるため、目的に応じ都度検討する必要がある

■体制検討時のポイント

■CSIRTをプロジェクトマネージャと位置づけ、「サイバー攻撃」に対しての演習を実現するとよい

⑩マネジメントだけでなく、実質的な企画運営まで全て行うケースが多い

■CISO/CROや上級のマネージャをプロジェクトオーナーとすることにより、プロジェクトに”お墨付き”を与え、関係者との調整を効果的に行えるようにする

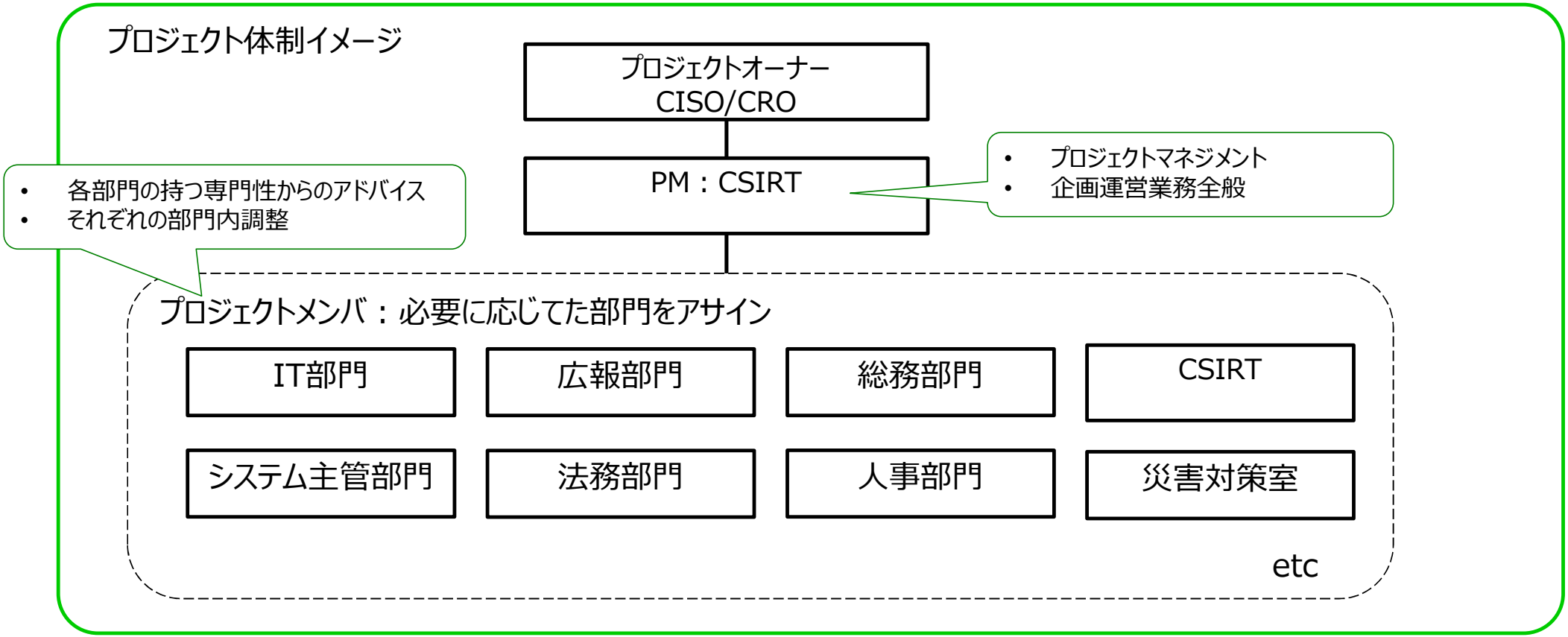
■自組織内の各部門からプロジェクトメンバへのアサイン

⑩各部門の持つ専門性からCSIRTとは別の視点でアドバイスしてもらえる

⑩部門間調整の窓口として活躍してもらえる

STEP1
プロジェクトイメージ

■CSIRTを中心とする体制により、「サイバー攻撃」への演習/訓練を実施するプロジェクトとする



STEP2
情報収集

STEP2
情報収集

- サイバー攻撃演習/訓練を実施するための情報収集を実施する
- これらの情報を「STEP3：サイバー攻撃演習/訓練計画の作成」「STEP4:シナリオ検討」のインプットとする
- 情報が全て集まらないと、サイバー攻撃演習/訓練が実施できないというわけではない

収集する情報

1. インシデント対応体制
2. インシデント対応フロー
3. ビジネスへの影響度
4. 自組織の規程
5. システム構成/ネットワーク構成
6. 自組織のセキュリティ関連情報
7. サイバー攻撃のトレンド
8. スケジュールのマイルストン

STEP2
情報収集1：インシデント対応体制

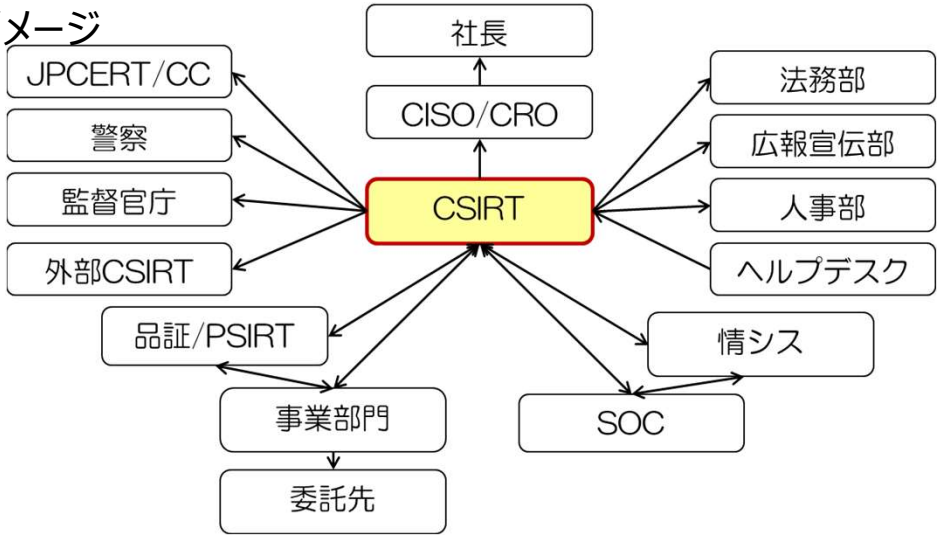
■インシデント対応における関係者を把握するためインシデント対応体制を把握する

■CSIRTの体制図等

■サイバー攻撃演習/訓練の参加者の選定のインプット

■シナリオの検討のインプット

インシデント対応体制イメージ



STEP2
情報収集2：インシデント対応フロー

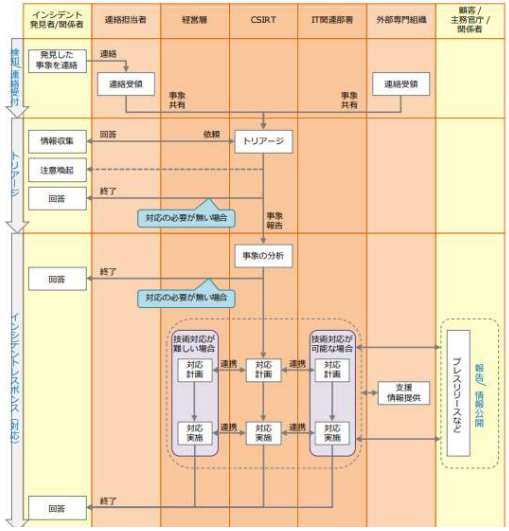
■インシデント対応フローはシナリオ作成のベースとなるため可能な範囲で準備する

■シナリオ作成のベースとしてのインプット

■状況付与の箇所のためのインプット

■サイバー攻撃演習/訓練の評価におけるベースラインとしてのインプット

インシデント対応フロー　イメージ



出展：JPCERT/CCインシデントハンドリングマニュアル

STEP2
情報収集3：ビジネスへの影響度

- インシデントが発生した時のビジネスへの影響度が大きいものは何かを把握する
- ビジネスへの影響度とシステムとの関連性を明確化し、シナリオ上でのインシデント発生個所のインプットとする

- 高い機密性が必要な情報
  - 個人情報
  - 資産管理区分に基づく情報
- 高い可用性が必要なシステム
- 高い完全性が必要な情報
- BCP対象となるシステム　etc.

STEP2
情報収集4：自組織の規程

■自組織の規程を確認し、インシデント発生時に行わなければならない行動を把握する

■セキュリティポリシー/プロシージャ/スタンダード
■個人情報保護規程
■BCP
■組織内のインシデントの報告基準/報告フォーマット
■ユーザー向けのインシデント対応マニュアル
■ISMS関連文書/Pマーク　等の自組織の取得するセキュリティ関連規格
■資産管理区分
■官公庁への報告基準　etc.

STEP2
情報収集5：システム構成/ネットワーク構成

■シナリオにリアリティを持たせるため、システム構成を把握する

- ■システムの把握
  - ■攻撃者のターゲットとなりやすいシステムの把握
    - ⑩機微な情報を持つシステム/外部公開サーバ/ActiveDirectory etc.
  - ■マルウェアのラテラルムーブメントができる領域の把握
  - ■特殊な運用を行っているシステム環境の把握
    - ⑩例：セキュリティアップデートを行えないシステム/例外的にUSBメモリを用いた運用を行っているシステム etc.
- ■システム運用の把握
  - ■システム運用体制
  - ■ログの種類、期間、保管方法　etc.
  - ■バックアップ状況　etc.
- ■導入しているセキュリティツールの把握
  - ■FW/IPS/EDR、外部SOC etc.

STEP2
情報収集6：自組織のセキュリティ関連情報

■シナリオにリアリティを持たせるため、自組織のセキュリティ関連情報を把握する

- ■過去に発生したインシデント
  - ■過去に発生したインシデントは、最もリアリティのあるシナリオのお手本
  - ■同等もしくは類似のインシデントをシナリオに活用
- ■リスクアセスメント結果
  - ■リスクアセスメント結果から、自組織によって発生しやすく影響度の大きいインシデントをシナリオとして検討
- ■インシデント対応上の課題
  - ■CSIRTの課題の確認
  - ■CISO/CROの課題の確認
  - ■その他インシデント対応部署の課題の確認
- ■その他、サイバー攻撃演習/訓練実施が必要な要因
  - ■官公庁や上位組織からの指示
  - ■自組織がサイバー攻撃を受ける可能性のある事象への対応
  - ■その他

STEP2
情報収集7：サイバー攻撃のトレンド

■サイバー攻撃のトレンドの情報を収集し、自組織に脅威となり得る攻撃をシナリオとして活用する

- ■攻撃手法の情報
- ■攻撃者の情報

- ■情報セキュリティ10大脅威：IPA
- ■各種セキュリティ関連セミナーでの情報収集
- ■NCAメンバとのディスカッション
- ■セキュリティ関連団体からの情報　etc.

STEP2
情報収集8：スケジュールのマイルストン

■スケジュールのマイルストンは明確に把握し、プロジェクトのスケジュールを具体化する

【スケジュールのマイルストンの例】

■経営層からの意向

■年度計画

■官公庁からの指示

■インシデントの再発防止としての期限

■その他

STEP3
計画の作成

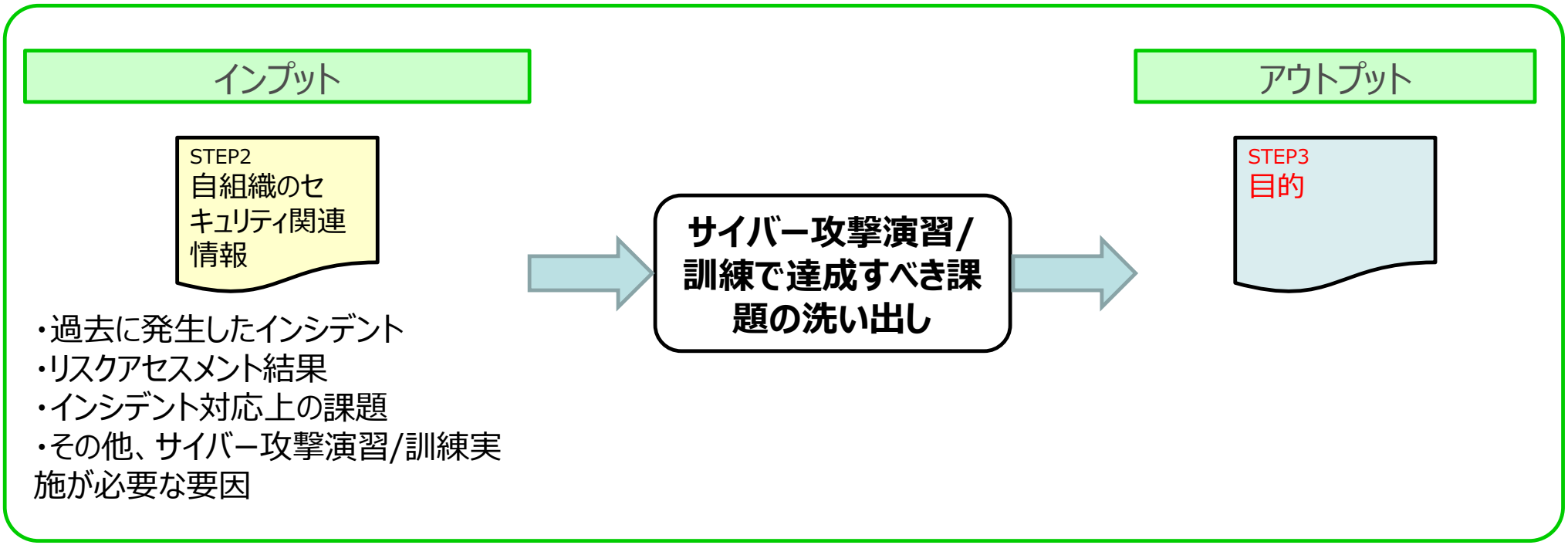
STEP3
計画の作成

■STEP2で収取した情報を元に、サイバー攻撃演習/訓練の計画を作成する

1. 目的
2. スコープ
   - ■対象システム
   - ■参加者
3. サイバー攻撃演習/訓練方式
4. スケジュール

STEP3
計画の作成1:目的

- サイバー攻撃演習/訓練の目的を明確化する
- 目的にあわせてシナリオ検討を行う



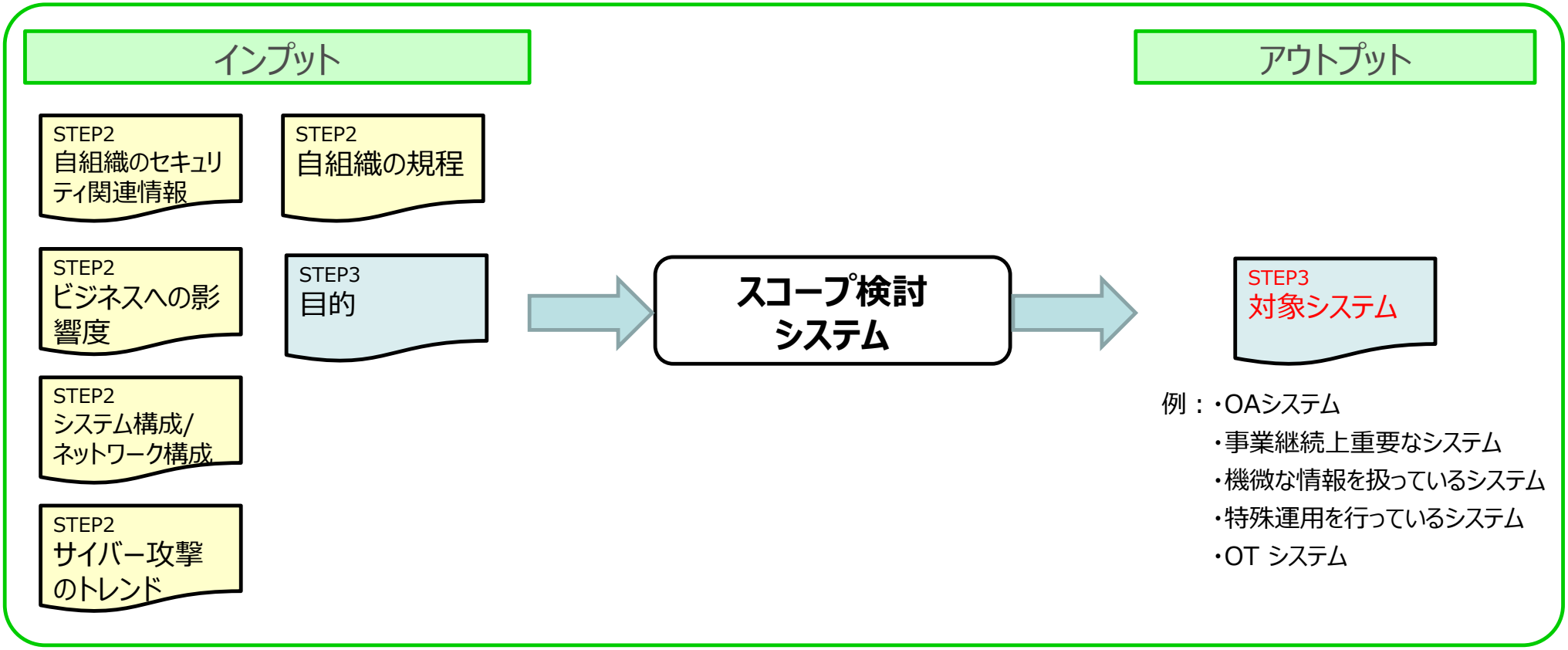
STEP3
計画の作成1:目的例

■主なサイバー攻撃演習/訓練の目的例は以下のとおりである

- ■インシデント対応フローの検証
- ■インシデント対応フローの習得
- ■サイバー攻撃における、事業継続計画(BCP)の検証
- ■CSIRTのインシデント対応能力の向上
- ■インシデント対応時の自組織内の情報連携の検証
- ■インシデント対応時の組織外情報連携の検証
- ■インシデント対応時のリソースの検証
- ■インシデント対応時のコミュニケーションツールの検証
- ■インシデント対応時のコミュニケーションツールの習得
- ■自組織内への啓発活動/意識向上/役割理解促進
- ■テクニカルスキルの習得　etc.

STEP3
計画の作成2:スコープ(対象システム)

■シナリオ上でのインシデントを発生させるシステムの定義を行う



STEP3
計画の作成2:スコープ(参加者)

■サイバー攻撃演習/訓練の参加者を決定する

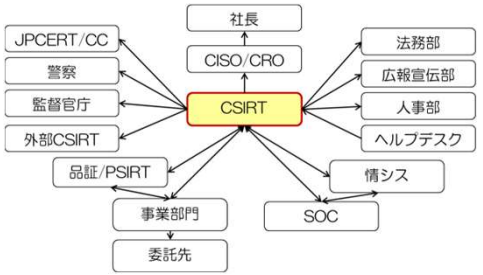
インプット

- STEP2 自組織のセキュリティ関連情報
- STEP2 インシデント対応体制
- STEP2 ビジネスへの影響度
- STEP2 自組織の規程
- STEP2 システム構成/ネットワーク構成
- STEP3 目的
- STEP2 サイバー攻撃のトレンド
- STEP3 対象システム

参加者の検討

アウトプット

STEP3
参加者



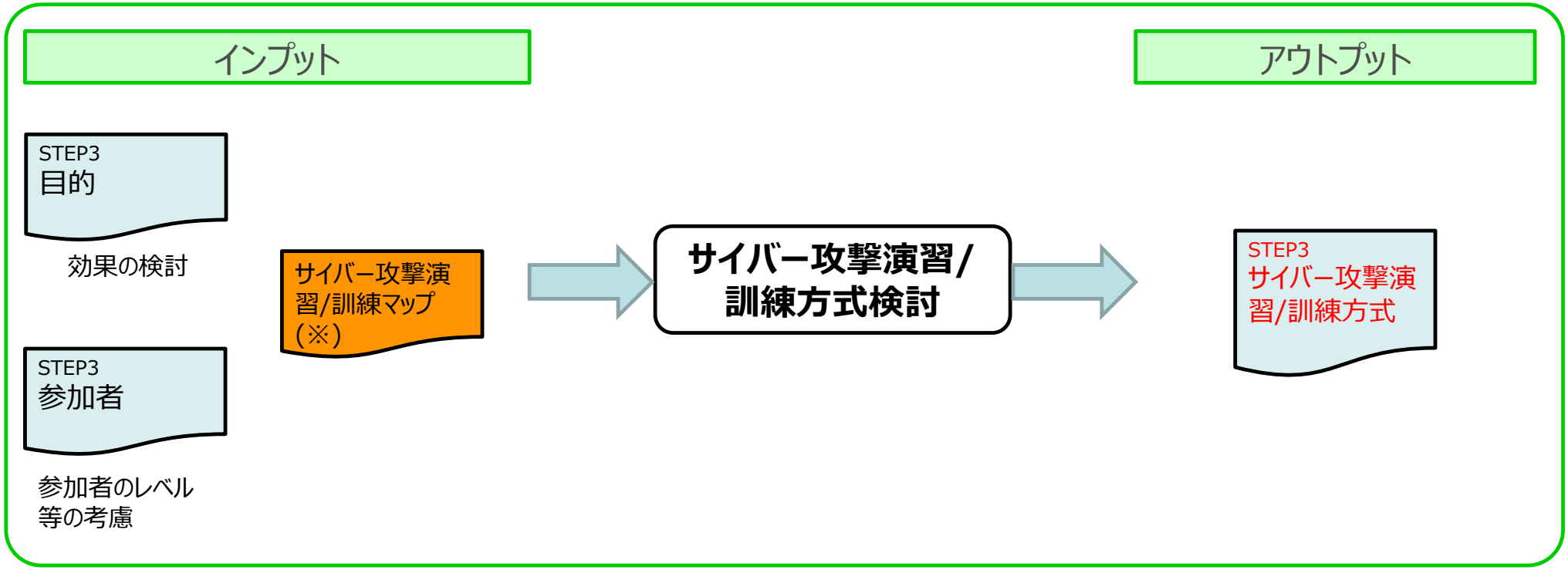
スコープ：参加者の選定　Tips

- 経営陣に近い上位者ほどリスク管理が論点となり、一方、現場に近い実対応者ほど技術的な論点となりやすいため、目的に合わせた参加者の選定が必要である
- 目的とシナリオによっては、活発なアクションを必要とする「メインの参加者」と、活躍の場が少ない「メイン以外の参加者」に分かれてしまう場合がある
  - 「メイン以外の参加者」から不満が出やすいので注意が必要
  - 「メイン以外の参加者」には、目的、役割を事前に伝え、活躍の場が少ないことを了承してもらった上で、参加し協力してもらうことを事前調整しておくことが重要である

  「メイン以外の参加者」の例：技術的な論点が多い場合の広報部門や総務部門等
- サイバー攻撃演習/訓練を初めて実施する場合などは、参加者を絞って実施(CSIRT内だけで実施)することにより、運営を円滑に実施できる場合がある。

STEP3
計画の作成3:サイバー攻撃演習/訓練方式

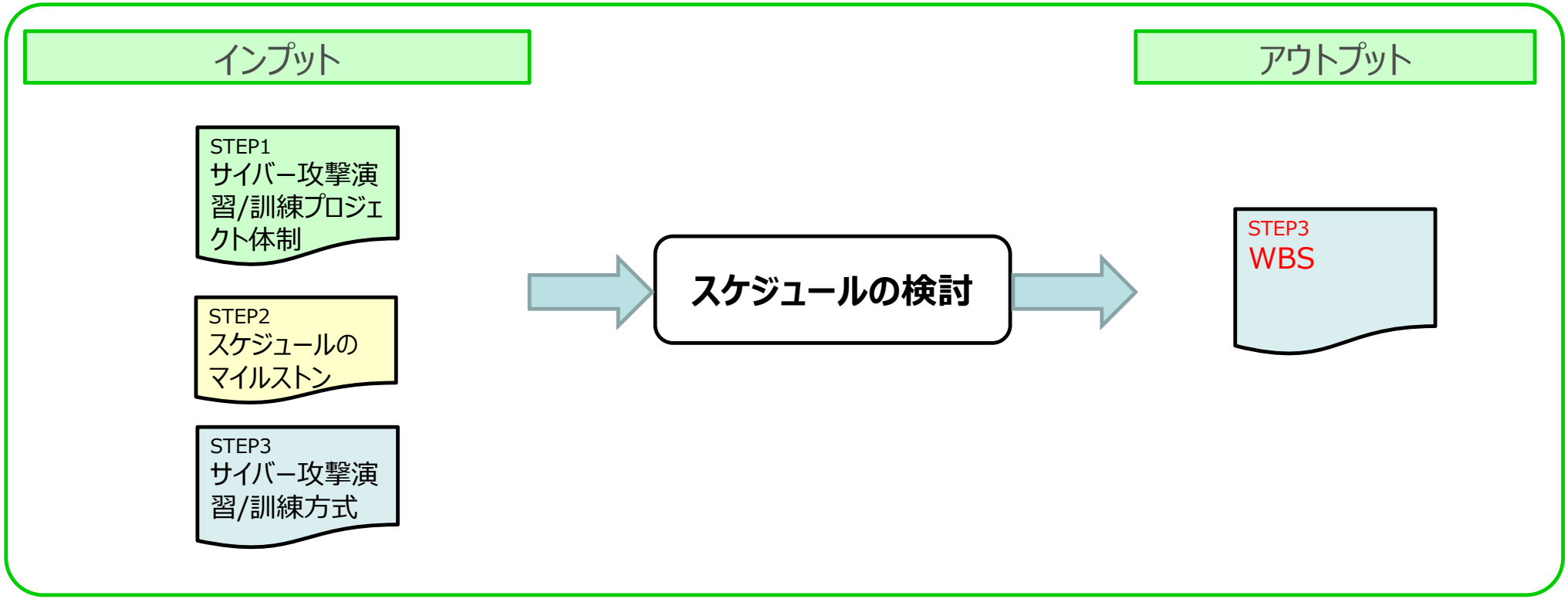
■どのようなサイバー攻撃演習/訓練方式を実施するかを検討する



※第3章参照

STEP3
計画の作成4:スケジュール

■サイバー攻撃演習/訓練実施をスケジューリングしWBSを作成する



STEP3
計画の作成4:スケジュール例

■サイバー攻撃演習/訓練のスケジュールをWBSとしてまとめる

【WBSイメージ】

項目		担当	スケジュール
シナリオ検討	シナリオ検討	CSIRT	
	状況付与テーブル検討	CSIRT	
	状況付与作成	CSIRT	
	レビュー	CSIRT、広報、総務、法務	
開催準備	日程調整/招待	CSIRT	
	タイムテーブル作成	CSIRT	
	設備準備	CSIRT	
	シミュレーション	CSIRT、広報、総務、法務	
実施		CSIRT	
評価		CSIRT	

STEP4
シナリオ検討

STEP4
シナリオ検討の項目

■シナリオ検討は以下の4項目で実施する

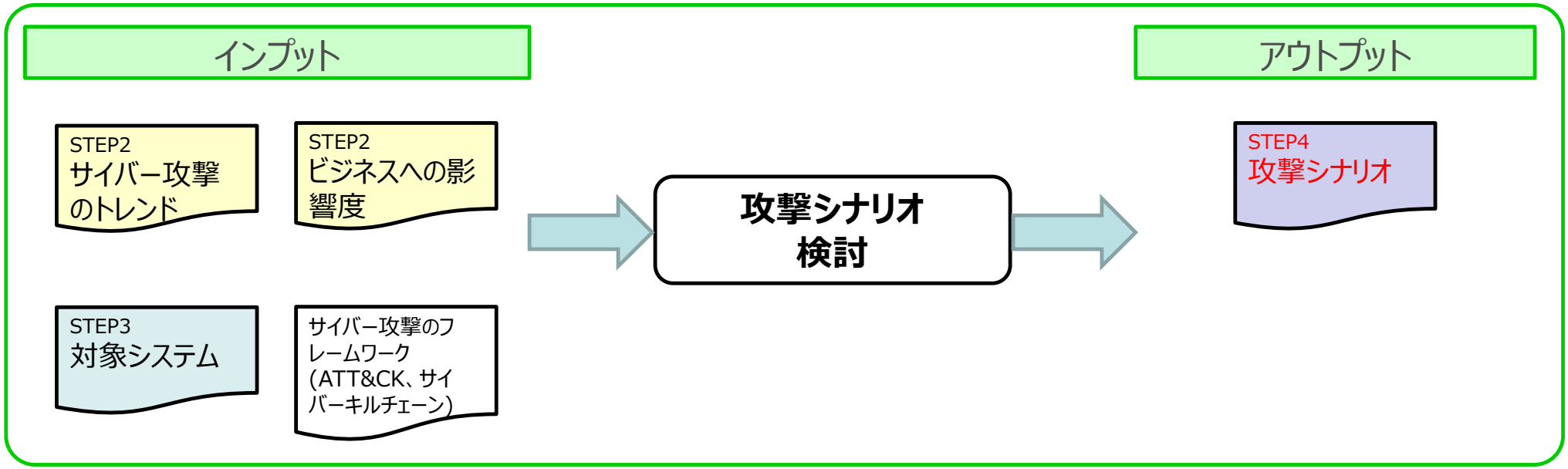
1. 攻撃シナリオ検討
2. 状況付与テーブル検討
3. 状況付与作成
4. レビュー

STEP4
シナリオ検討1：攻撃シナリオ検討

■攻撃者の観点で、どのようにシステムを侵害していくかを検討する

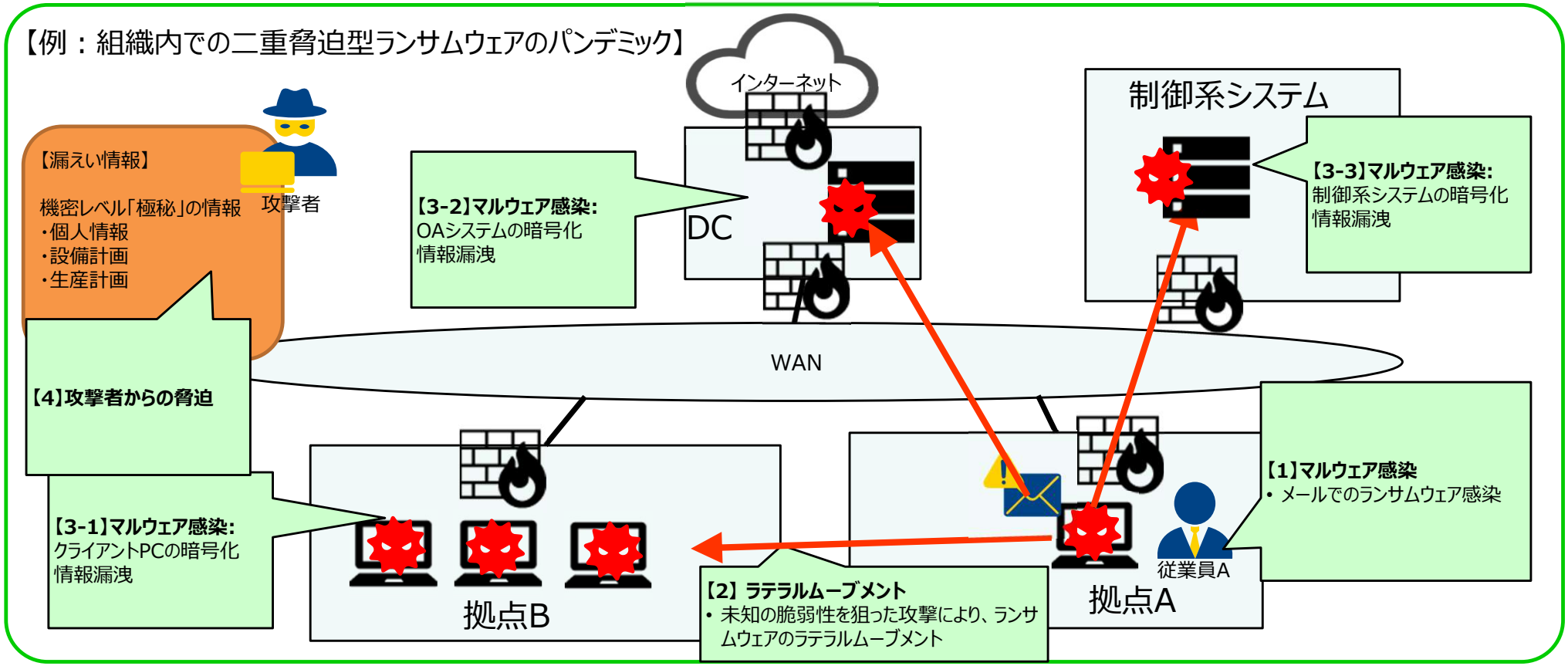
■サイバー攻撃のフレームワーク(ATT&CK、サイバーキルチェーン)等を参考にすることにより、攻撃シナリオに具体性を持たせられる

■攻撃者(組織・人物像、目的等)を攻撃シナリオのバックボーンとして検討すると、攻撃シナリオのイメージを膨らませることができる



STEP4
シナリオ検討1： 攻撃シナリオ検討例

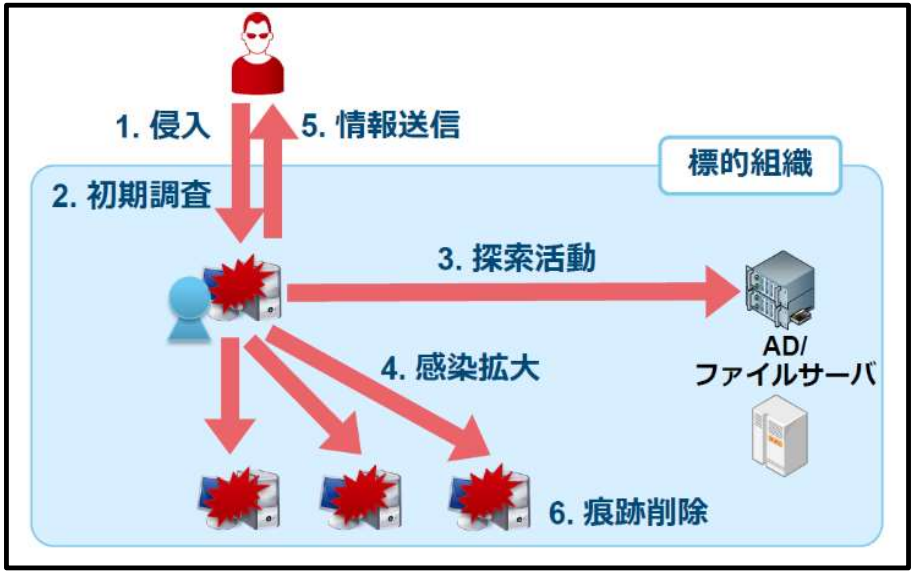
- 攻撃者がどのように攻撃を行うかを明確にする
- 自組織のシステムを考慮し、可能な限り現実味のある攻撃シナリオを作成する



STEP4
シナリオ検討1： 攻撃シナリオ検討 フレームワーク

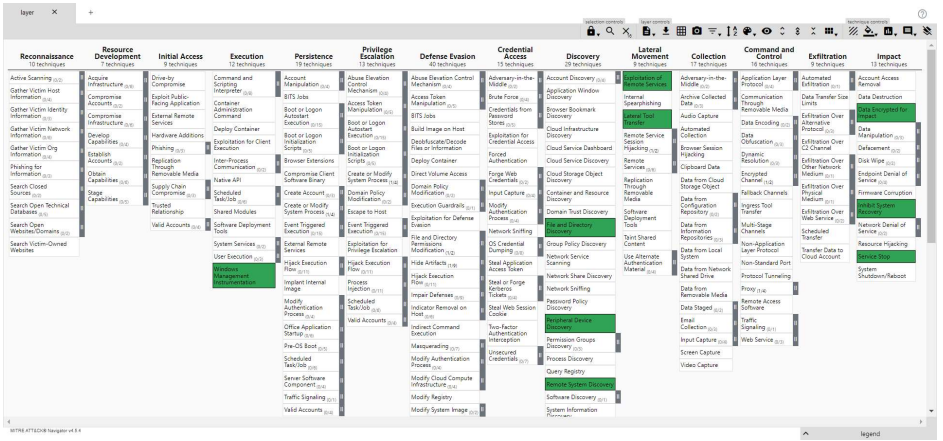
■サイバー攻撃に関するフレームワークを参考とし、攻撃シナリオの検討を実施することは有効である

サイバーキルチェーン



出典：JPCERT/CC Log Analysis Training

MITRE ATT&CK



https://mitre-attack.github.io/attack-navigator/

STEP4
シナリオ検討1： 攻撃シナリオ検討　Tips

Tips(1)　シナリオ作成の参考

■大規模セキュリティインシデントなどでの公開されたインシデントレポートを参考にして、自組織へ当てはめた場合にどうなるか等を検討することにより、シナリオ作成を効率的に実施できる場合がある

Tips(2) 悪いシナリオ

■自社では発生し得ないシナリオ
- ■自社と異なる業種を想定したシナリオ（例：製造業でオンラインバンキングサイトの侵害）
- ■自社のシステム構成上、絶対に起こりえないようなシナリオ

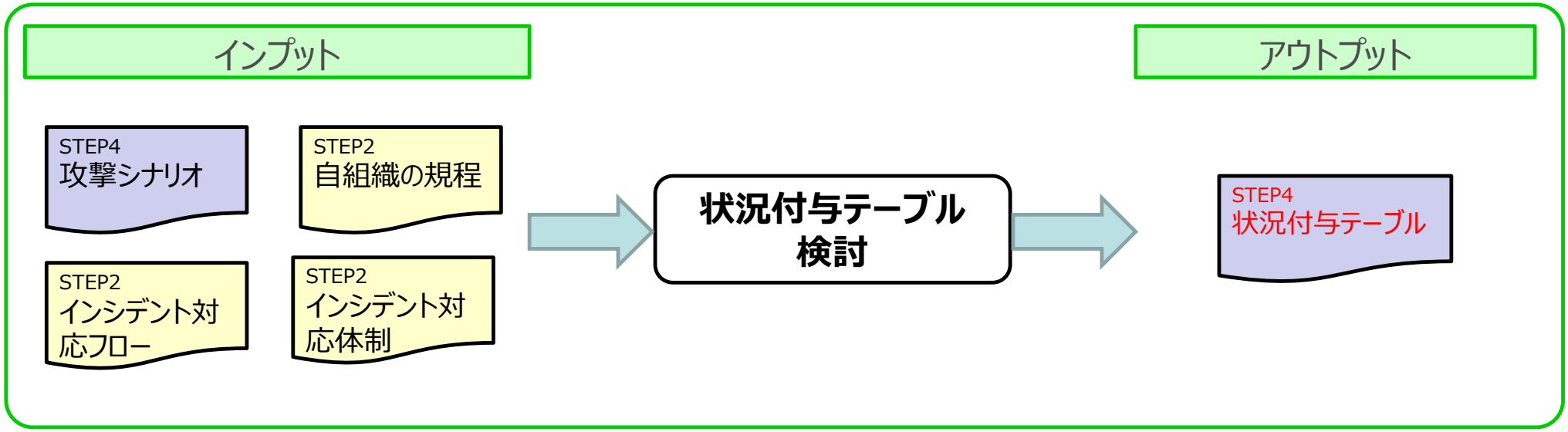
■流行から廃れてしまったシナリオ
- ■想定する攻撃者の動機付けが希薄なシナリオ（愉快犯的なサイト改ざん、ハクティビストによる脅迫等）
- ■既に世間的に対策が取られていてあまり重要な問題にならないシナリオ

■対応が手詰まりになるシナリオ
- ■攻撃が沈静化するのを待つしかないシナリオ（DDoS攻撃のシナリオ等）

■演習終了後にモヤモヤ感が残るシナリオ
- ■原因が分からず、解決の方策も見いだせないまま終わるシナリオ

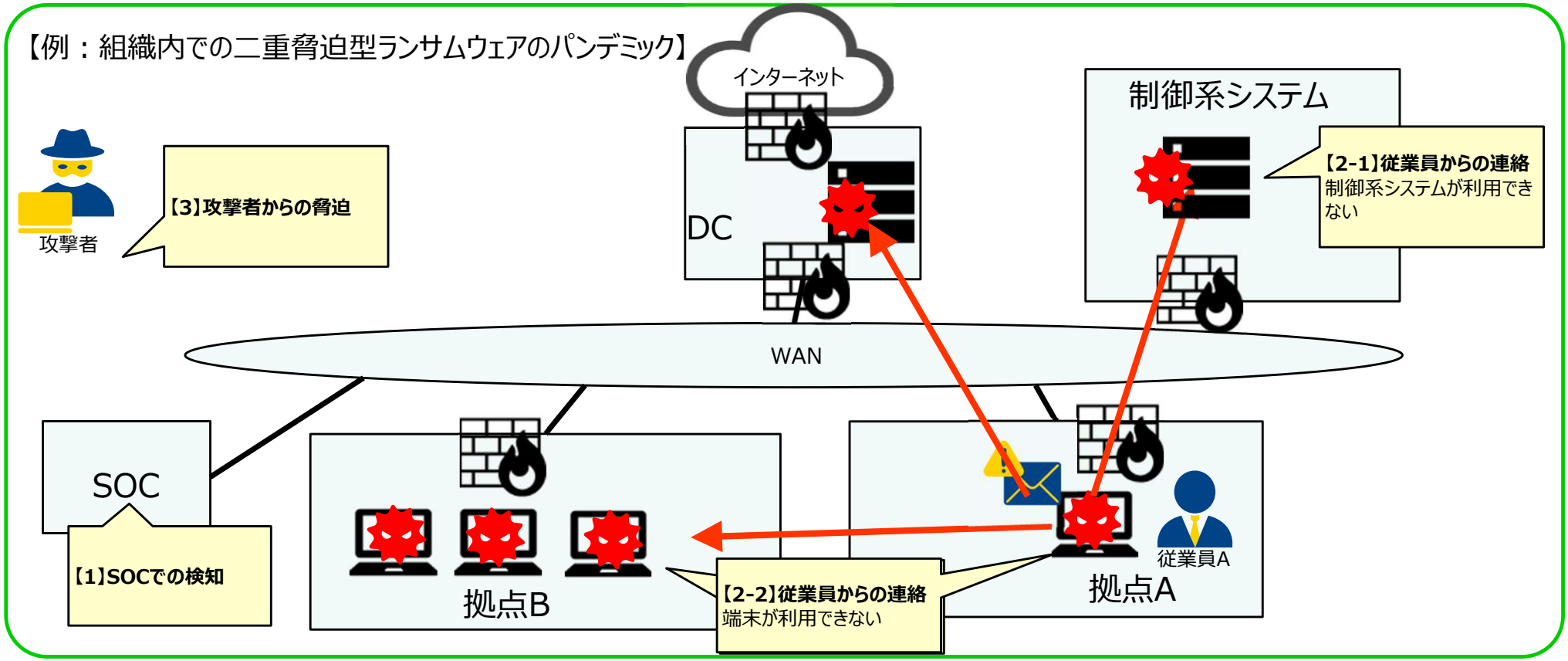
STEP4
シナリオ検討2：状況付与テーブル検討

- 「攻撃シナリオ」と対比し、サイバー攻撃の検知や対応等の状況付与を検討し、テーブルとして取りまとめる
- 参加者への提供する情報の概要を設計する
- 「シナリオ上の時間」も明確にする



STEP4
シナリオ検討2：状況付与テーブル検討方法(1/3)

■攻撃シナリオを、防御側からの視点で逆トレースを行い、状況付与テーブルとして作成する

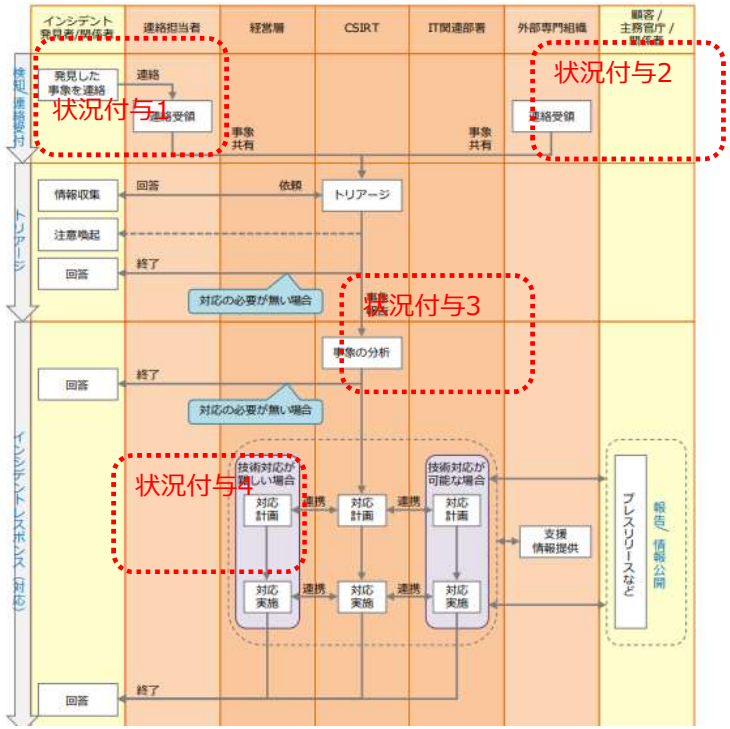


STEP4
シナリオ検討2：状況付与テーブル検討方法(2/3)

■状況付与テーブルを自組織のインシデント対応フローに当てはめて机上検証する

■インシデント対応におけるフェーズ(検知、初動対応、分析、封じ込め etc.)からバランスよく状況付与できるように検討する

状況付与検討イメージ



出展：JPCERT/CCインシデントハンドリングマニュアル

STEP4
シナリオ検討2：状況付与テーブル検討方法(3/3)

■サイバーレジリエンスを持たせるため、以下の観点で検討する

	因子	状況付与の例
予測力	潜在的な脅威の因子 （予測が難しい状況）	• 漏洩情報に顧客の情報が含まれていた • システムにより顧客の業務にも影響が波及
耐性力	ストレス因子	• マルウエア感染の拡大が進行中 • 顧客/ユーザからの多数のクレーム • 経営や社内関係者からの問合せ
回復力	影響を拡げる因子 回復を阻害する因子	• マルウエアが潜伏している可能性 • バックアップにも影響は波及し、復旧が困難
適応力	適応を阻害する因子	• パッチを適用したらシステムが動作しなくなるのですぐには対応できないとの回答 • システムを改修するための予算が無い

STEP4
シナリオ検討2：状況付与テーブル例

■状況付与テーブルとして一覧化する
- ■付与時間
- ■状況付与
- ■期待するアクション

状況付与テーブルイメージ

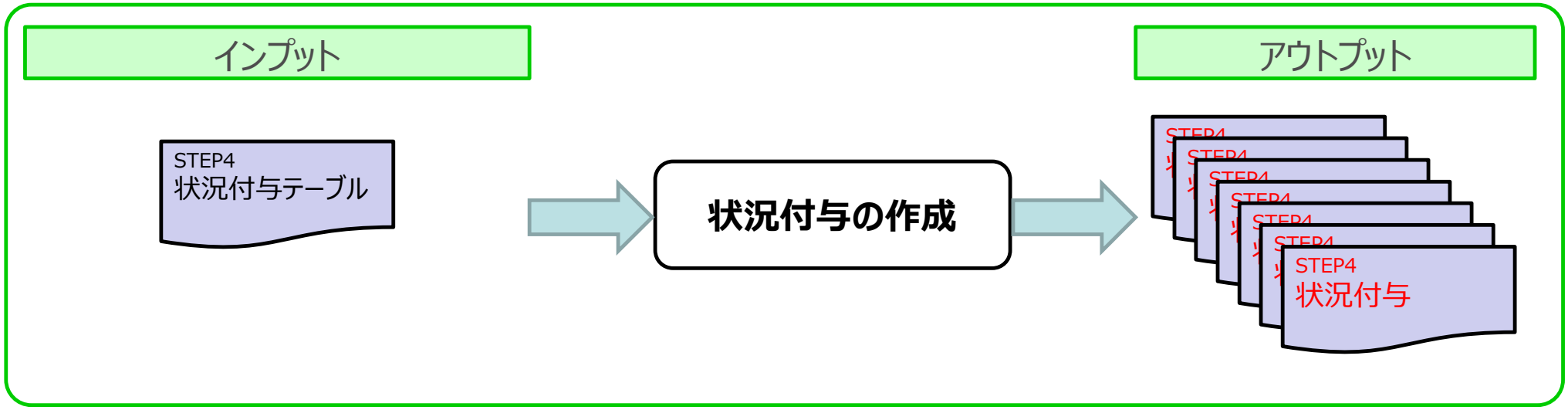
状況付与に関する記述

以下より期待するアクションの洗い出し
- インシデント対応体制
- インシデント対応フロー
- 自組織の規程

項番	付与時間	状況付与			期待するアクション	備考
		シナリオ上の日時	概要	内容		
1	xx:xx	○月○日 yy:yy	SOCでの検知	SOCでのマルウェア感染の検知を受ける アラートレベル：Critical	・SOCへの詳細情報の確認 ・ユーザへの連絡 ・初動対応としての隔離の実施	
2	xx:xx	○月○日 zz:zz	ユーザからのヒアリング	・メール添付を開いた ・現状はネットワークから切り離し済 ・保持している情報 ・個人情報　○○件	• 端末の確保 • エスカレーション • 詳細分析実施判断	インシデント対応フロー　P○○
3	xx:xx	….	….	….	….	….

STEP4
シナリオ検討3：状況付与作成

■参加者に提示できるプレゼン形式で状況付与を作成する



STEP4
シナリオ検討3：状況付与例

■状況付与のイメージは以下のとおりである

X月X日(水) XX:XX

サイバー攻撃演習/訓練における想定の時間

参加者の検討時間

検討時間	10分

状況付与(No.1)

✓ 「従業員A」より「制御システムが止まって生産できない。システムファイル名がおかしくなっており、セキュリティインシデントの可能性がある」とCSIRTへ問合せの入電を受ける。

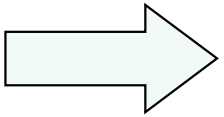
状況付与における客観的な事実のみの記載

ヒント：

① この時点でどのような対応をしますか？
② インシデントレベルは何になりますか？
③ どこにエスカレーションしますか？
④ インシデントレベル決定後は、どのような対応をしますか？

参加者のレベルによってヒントを記載

従業員A



CSIRT

提示タイミング	13:15

状況付与の提示タイミング

STEP4
シナリオ検討4：レビュー

■有識者や関係者等によるレビューを実施し、品質の向上を行う

■シナリオへのレビュー
- ■目的を達成できるものか？
- ■シナリオ自体に無理がないか？
- ■シナリオに補足したほうがよい観点はないか？
- ■etc.

■状況付与へのレビュー
- ■内容は十分で、参加者にわかりやすいものか？
- ■非現実的な状況付与ではないか？
- ■状況付与するタイミングや時間配分は適切か？
- ■付与する情報に過不足はないか？
- ■スライドは見やすいか？
- ■etc.

■期待するアクションのレビュー
- ■他に期待するアクションがないか？
- ■インシデント対応フローとあっているか？
- ■etc.

STEP5
実施準備/実施

STEP5
実施準備/実施

■今までの計画を元に実施準備を整え実施する

1. 日程調整/招待
2. タイムテーブル
3. 設備準備
4. シミュレーション
5. サイバー攻撃演習/訓練実施

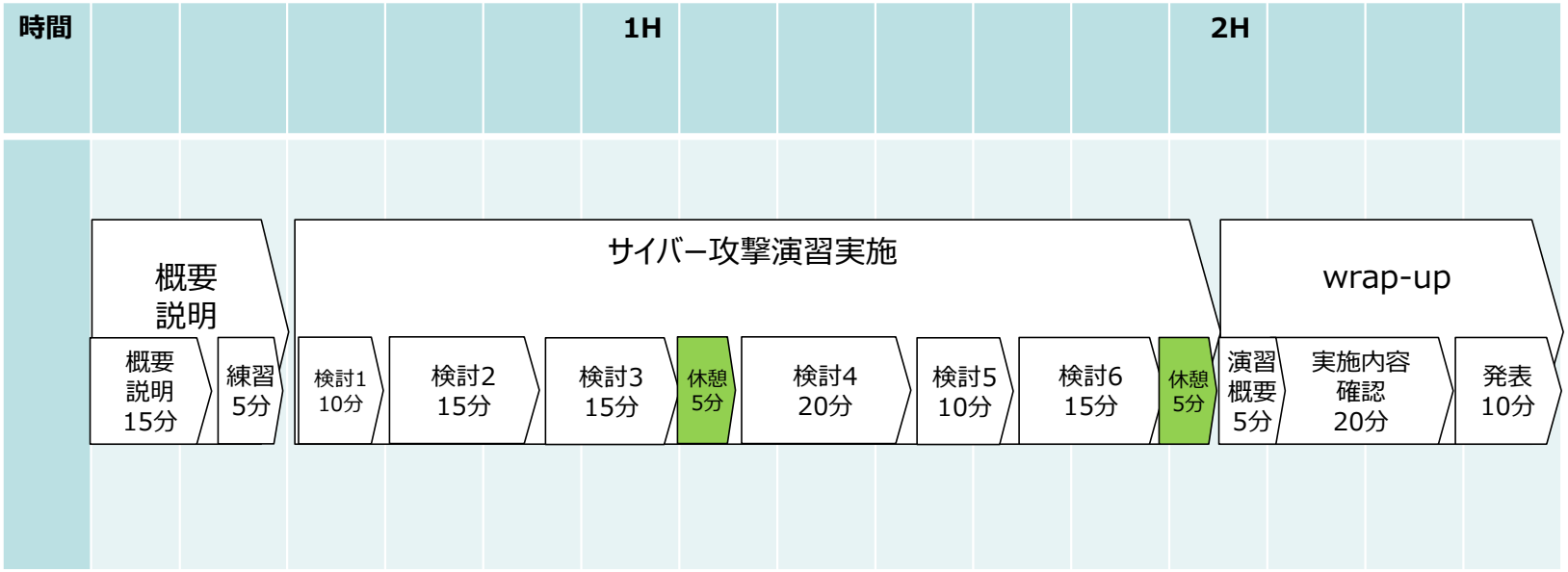
STEP5
実施準備/実施1:日程調整/招待

- 参加者やプロジェクトメンバ等の日程調整を実施する
- 参加者への招待を実施し、開催に備える

STEP5
実施準備/実施2:タイムテーブル

■サイバー攻撃演習/訓練のタイムテーブルを作成する

【タイムテーブルイメージ】



STEP5
実施準備/実施3:設備準備

■サイバー攻撃演習/訓練に必要な設備を洗い出し、準備を整える

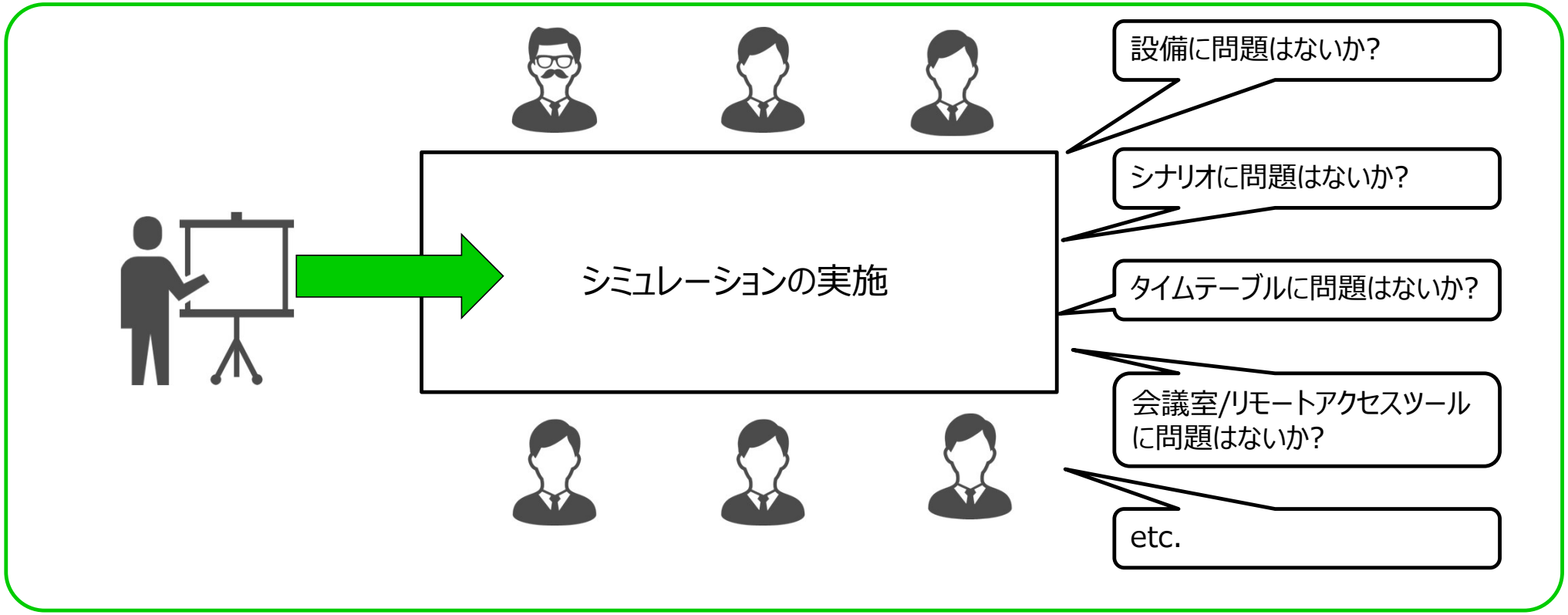
【設備例】

■会議室
■リモートアクセスツール
■マイク
■ホワイトボード
■プロジェクタ
■テーブル/椅子
■ビデオカメラ
■投影用PC etc.

STEP5
実施準備/実施4:シミュレーション

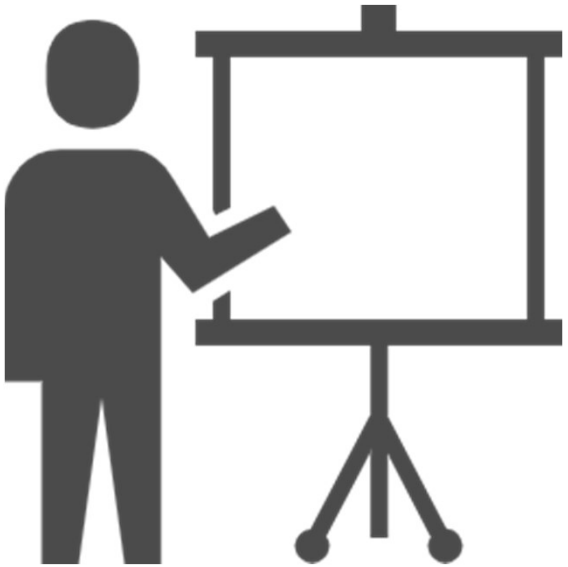
■サイバー攻撃演習/訓練プロジェクト内でシミュレーションを実施し、最終確認を実施する

■できるだけ本番環境に近い状況で実施する



STEP5
実施準備/実施5:サイバー攻撃演習/訓練実施

■ここまで準備が整えば、開催当日にサイバー攻撃演習/訓練を実施するだけ！



STEP6
実施後対応

STEP6
実施後対応　概要

■サイバー攻撃演習/訓練実施後対応は以下の内容を実施する

1. 評価
2. フォローアップ

STEP6
実施後対応1:評価

■サイバー攻撃演習/訓練の評価は以下の4軸で検討

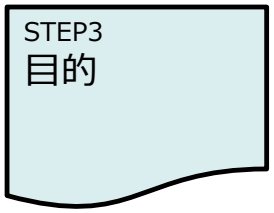
■全ての評価が必要ではない。必要に応じて選択

(1)目的達成度評価
(2)参加者評価
(3)インシデント対応評価
(4)第三者評価
(5)運営評価

STEP6 実施後対応1:評価
(1).目的達成度評価

■「目的が達成できたかどうか」を評価する

【イメージ】



■目的：インシデント対応プロセスの改善

■評価結果：

訓練により、インシデント対応プロセスの改善点が●●件発見された。本演習の目的が達成できた。

本演習結果をもとに、インシデント対応フローの改善を○○までに実施する予定である

STEP6 実施後対応1:評価
(2).参加者評価

- 参加者による評価はアンケートを用いる
- アンケートは早い段階(即時～1週間以内)の回収が望ましい
- 改善点だけではなく、良かった点も記載するアンケートにすると、CSIRTのモチベーションがあがり、長所を伸ばす改善ができる

- アンケートの項目例
  - サイバー攻撃演習/訓練自体の満足度
  - 気づき
  - 今後の業務に役に立つか/どのような業務に役に立つか
  - 積極的に参加できたか
  - サイバー攻撃演習/訓練自体の改善点　etc

STEP6 実施後対応1:評価
(3).インシデント対応評価

■参加者の演習/訓練中でのインシデント対応の正確性を評価する

■可能であれば、参加者の理解の促進につながるため演習終了直後に実施することが望ましい

- ■シナリオ作成時に検討した「期待するアクション」との対比
- ■インシデント対応マニュアル/フロー/チェックリストからの対比
  - ■記載内容を網羅的に実現できていたか
  - ■帳票類の存在を意識して、適切に利用できていたか
- ■インシデント対応経験豊富なメンバによる確認
  - ■適切なコミュニケーションをとれていたか
  - ■適切な判断ができていたか
  - ■インシデント対応上、NGな行為をしていなかったか
    - ⑩証拠を消すような対応
    - ⑩インシデントを拡大させるような対応　等

STEP6 実施後対応1:評価
(4).第三者評価

- 第三者による客観的な評価を受ける
- 第三者は、自組織内外問わない

【第三者評価のメリット】

- 自組織内では得られない着眼点での評価の期待
- 専門性からの評価
- 他組織と比較しての評価

STEP6 実施後対応1:評価
(5).運営評価

■サイバー攻撃演習/訓練実施の運営に関して評価を実施する

■次回のサイバー攻撃演習/訓練実施に向けて、より効率的に実施できるところはないか考察する

■定量評価を行うことは非常に難しい。成果を鑑みての定性的な評価となる

- 目的を達成するのに十分な運営ができたか
- 検討期間は適切だったか
- 準備稼働は適切だったか
- コストに見合う成果はあったのか
  - 業務委託費は適切だったか
- WBSは適切だったか
- プロジェクト体制は適切だったか
  - etc

STEP6
実施後対応2:フォローアップ

■サイバー攻撃演習実施後に、洗い出された課題に対しての改善に関するフォローアップを実施する。

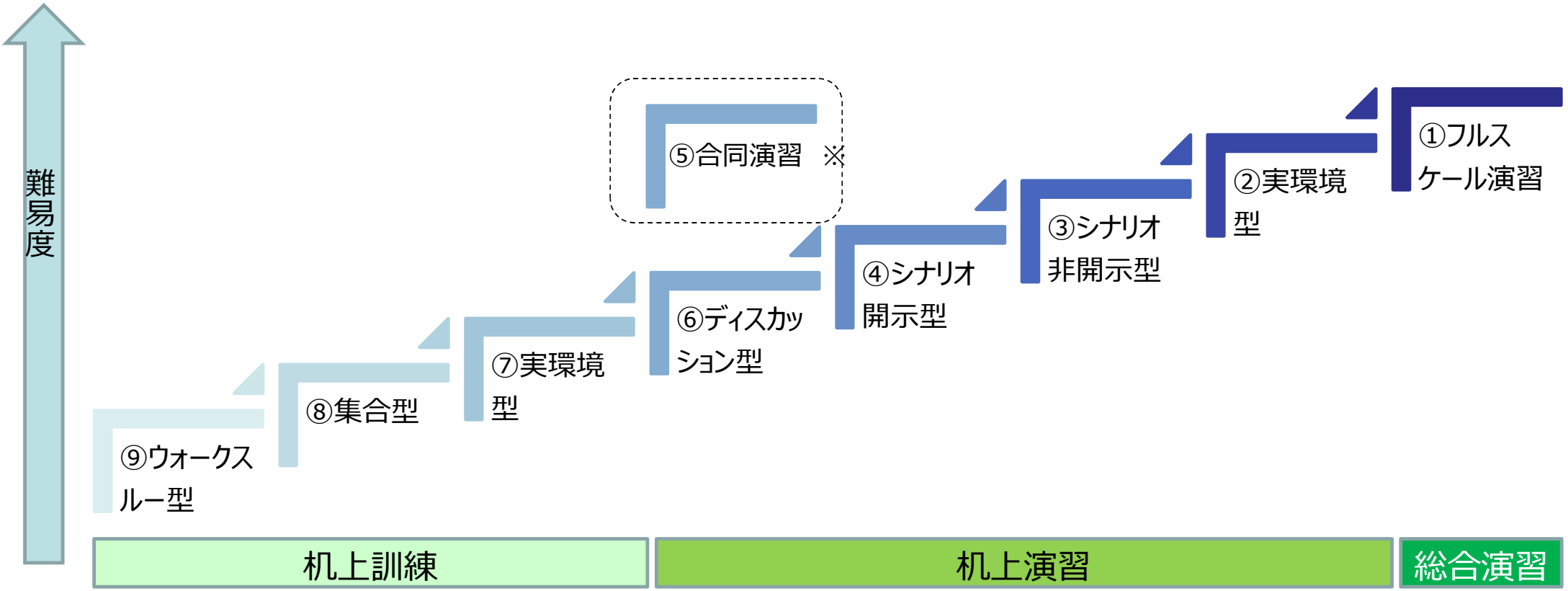
- ■課題の明確化の実施
- ■改善計画の策定
  - ■改善実施の主体の明確化
  - ■スケジューリング
  - ■改善計画の経営層等への承認
- ■フォローアップ
  - ■改善の進捗確認
  - ■改善内容の確認
- ■参加者への事後におけるインタビュー　等

※本ページは「演習」におけるアプローチとなる

第3章
サイバー攻撃演習/訓練マップ

サイバー攻撃演習/訓練マップ

■ロールプレイ型のサイバー攻撃演習/訓練には以下のタイプに分別される



※合同演習は、複数組織が同時に演習を実施する特徴がある

サイバー攻撃演習/訓練マップ：難易度の定義

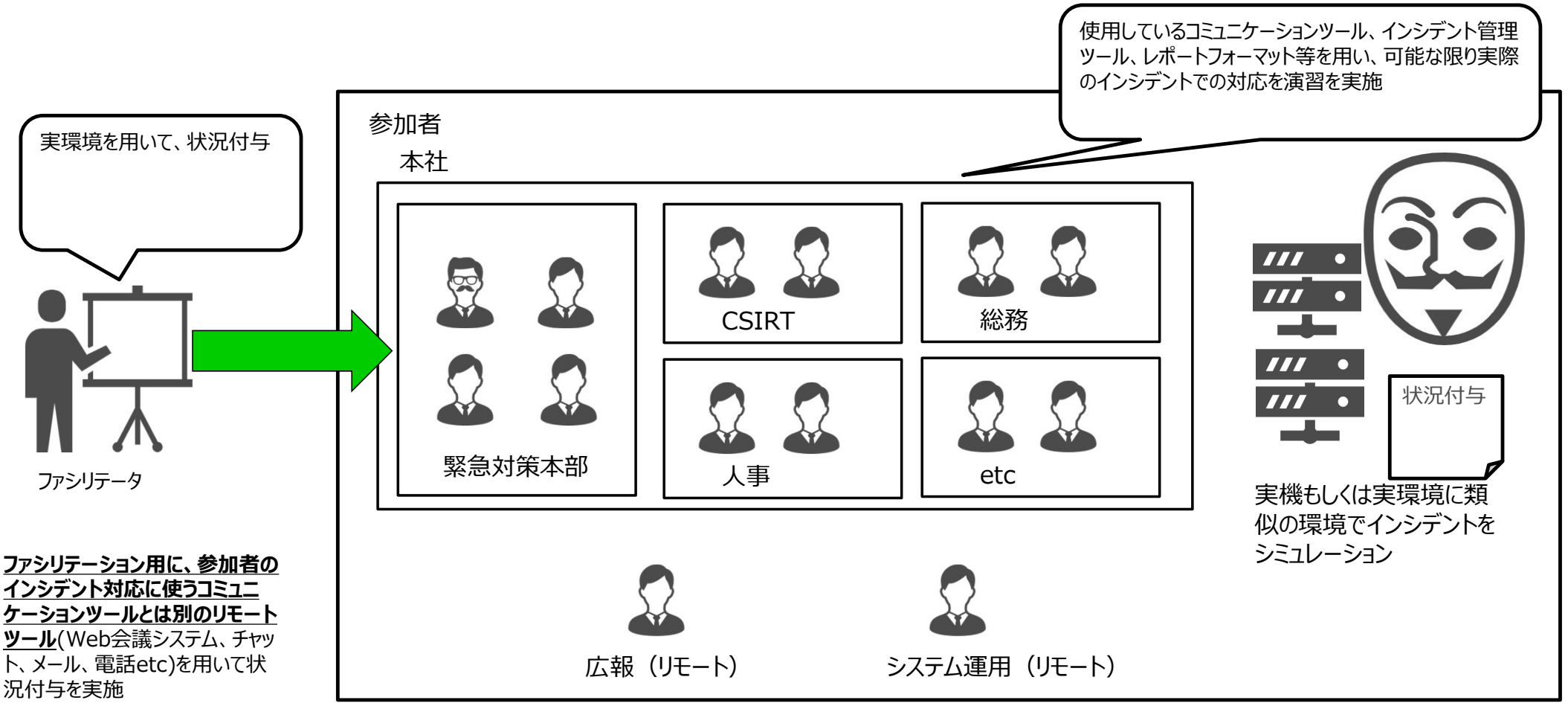
■ サイバー攻撃演習/訓練マップで定義する難易度は以下の通り

難易度	サイバー攻撃演習/訓練map	実施期間の目安	準備期間の目安	実施の難しさ	参加者に求められるレベル	ファシリテーションの難しさ
★★★★★	①フルスケール演習 ②机上演習：実環境型	1日 ～3日	6か月～	• 経営層を含む、自組織の全体に入念な調整が必要 • 設備的な調整が必要 • シナリオの検討内容が多岐にわたり、複雑になる	• 参加者がインシデント対応において、ビジネスへの影響度を鑑みて、インシデント対応フローを記載内容を超えた高度な判断が実施できる • 参加者がサイバー攻撃演習/訓練の経験が豊富である	• 経験豊富なファシリテータにて実施され、シナリオで定義していない不測の事態が発生したとしても臨機応変にサイバー攻撃演習/訓練を進行できる
★★★★	③机上演習：シナリオ非開示型	2時間 ～1日	3～6か月	• 組織全体に調整が必要 • シナリオの検討内容が多岐にわたり、複雑になる	• 参加者が定められた手順をベースとして、臨機応変な対応を実施できる • 参加者がサイバー攻撃演習/訓練の経験が豊富である	• シナリオの進行を鑑みて、適切なファシリテーションを実施できる
★★★	④机上演習：シナリオ開示型 ⑤机上演習：合同演習 ⑥机上演習：ディスカッション型	2時間 ～6時間	3～6か月	• 自組織内組織全体に調整が必要 • シナリオの検討に労力がかかる	• 参加者が定められた手順でのインシデント対応の経験があり、インシデント対応フローを理解している • 参加者がサイバー攻撃演習/訓練の参加経験がある	• 定められたシナリオを遂行できる • 参加者の様々な質問に対してその場で答えられる
★★	⑦机上訓練：実環境型 ⑧机上訓練：集合型	～2時間	3～6か月	• 自組織内組織全体に調整が必要 • シナリオの検討に労力がかかる	• 参加者がインシデント対応の経験が浅い • 参加者がインシデント対応フローを十分に理解していない • 参加者がサイバー攻撃演習/訓練の経験がない、もしくは浅い	• 定められたシナリオを遂行できる • 参加者の質問に別途検討のうえ回答できる
★	⑨机上訓練：ウォークスルー型	15分 ～60分	1日	• CSIRT内の簡易な調整のみで実行できる	• 参加者がインシデント対応の未経験者	• ファシリテータ不在でも実施可能 • 定められたシナリオを遂行できる

サイバー攻撃演習/訓練マップ①フルスケール演習

項目	内容
概要	• インシデント対応に関わる全ての参加者が参加する演習 • 実機もしくは実環境に類似の環境でインシデントをシミュレーションした対応を実施 • ログ解析等の技術的な対応も演習シナリオに組み込むことも可能 • 最も実践的な演習 • シナリオは参加者には非開示
想定参加者	• インシデント対応に関連する全メンバ (経営層/CSIRT/インシデント対応関連組織)
演習実施環境	• 参加者の業務環境
効果	• 最も実環境に近い状況で高いレベルでの組織的なインシデント対応力の実現 • 組織全体のインシデント対応能力の向上 • インシデント対応時に実際に活用するコミュニケーションツールの熟練度向上
難易度	★★★★★
備考	• 個別の業務形態により、実施方法の検討が必要 • 実環境での実施可否

サイバー攻撃演習/訓練マップ①フルスケール演習　イメージ



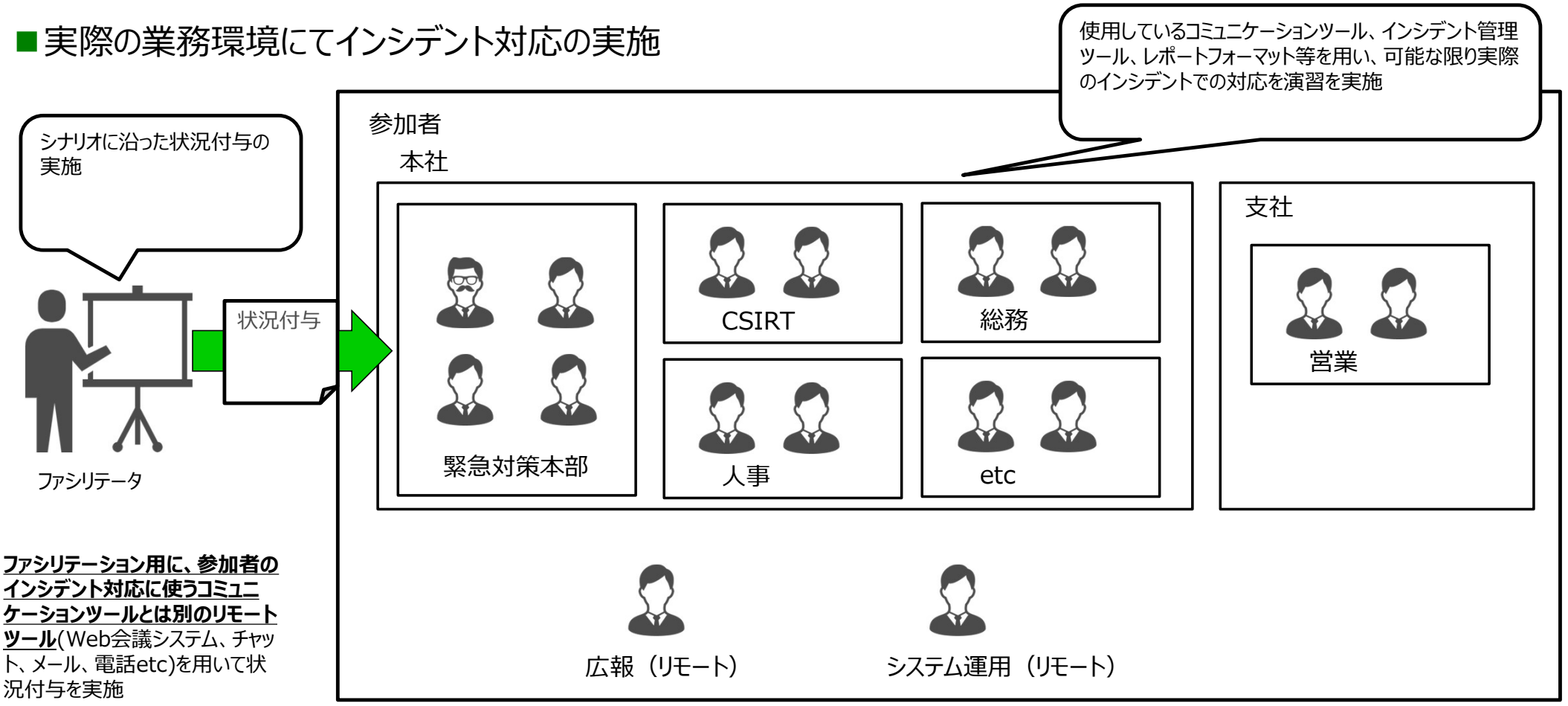
ファシリテーション用に、参加者のインシデント対応に使うコミュニケーションツールとは別のリモートツール(Web会議システム、チャット、メール、電話etc)を用いて状況付与を実施

サイバー攻撃演習/訓練マップ②机上演習：実環境型

項目	内容
概要	• 参加者は、実際に組織で用いるインシデント対応時に利用するコミュニケーションツール(電話、メール、チャット、リモート会議ツール、インシデント管理ツールetc)を用いて演習を実施 • ファシリテータによる状況付与によって演習を実施 • シナリオは参加者に非開示
想定参加者	• CSIRT • インシデント対応関連組織　etc
演習実施環境	• 参加者の業務環境
効果	• 高いレベルでの組織的なインシデント対応力の実現 • 組織全体のインシデント対応能力の向上 • インシデント対応時に実際に活用するコミュニケーションツールの熟練度向上
難易度	★★★★★
備考	• ファシリテータの状況付与に用いるコミュニケーション手段を、インシデント対応のコミュニケーションツールとは別で準備する必要性あり

サイバー攻撃演習/訓練マップ②机上演習：実環境型　イメージ

■実際の業務環境にてインシデント対応の実施

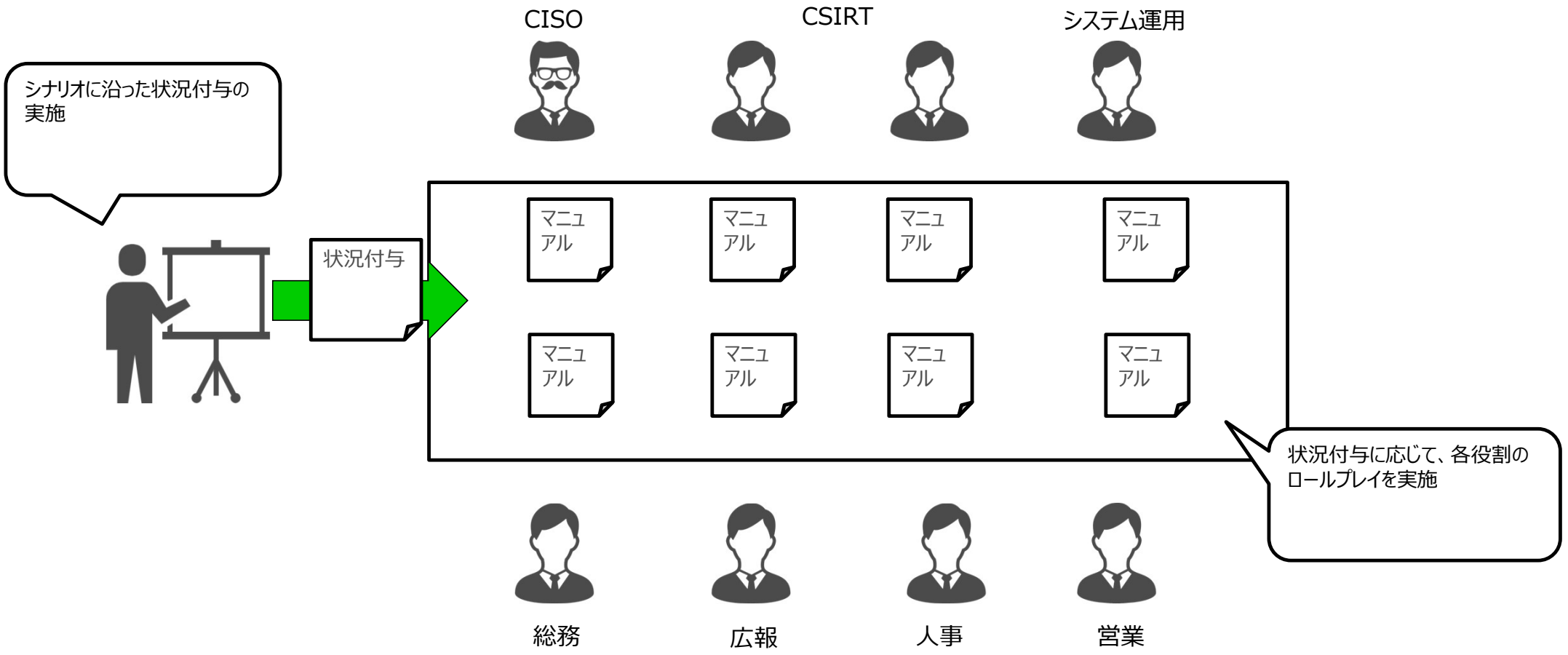


ファシリテーション用に、参加者のインシデント対応に使うコミュニケーションツールとは別のリモートツール(Web会議システム、チャット、メール、電話etc)を用いて状況付与を実施

サイバー攻撃演習/訓練マップ③机上演習：シナリオ非開示型

項目	内容
概要	• 参加者とファシリテータは会議室/リモート会議ツールにて集合して実施 • ファシリテータによる状況付与によって演習を実施。演習は主に会話によるコミュニケーションで実施 • 参加者は自身の知識・経験と既存のドキュメント(インシデント対応フロー等)を用いてロールプレイを実施 • シナリオは参加者には非開示
想定参加者	• CSIRT • インシデント対応関連組織　etc
演習実施環境	• 会議室/リモート会議ツール
効果	• 組織全体のインシデント対応能力の向上 • インシデント対応フローに表現しきれないような個別事象やイレギュラーな状況における、対応や判断能力の育成 • 演習によるインシデント対応経験
難易度	★★★★
備考	• 参加者のインシデント対応力によっては、演習が円滑に進まないリスクあり その場合にはファシリテータによるフォローを実施する必要あり

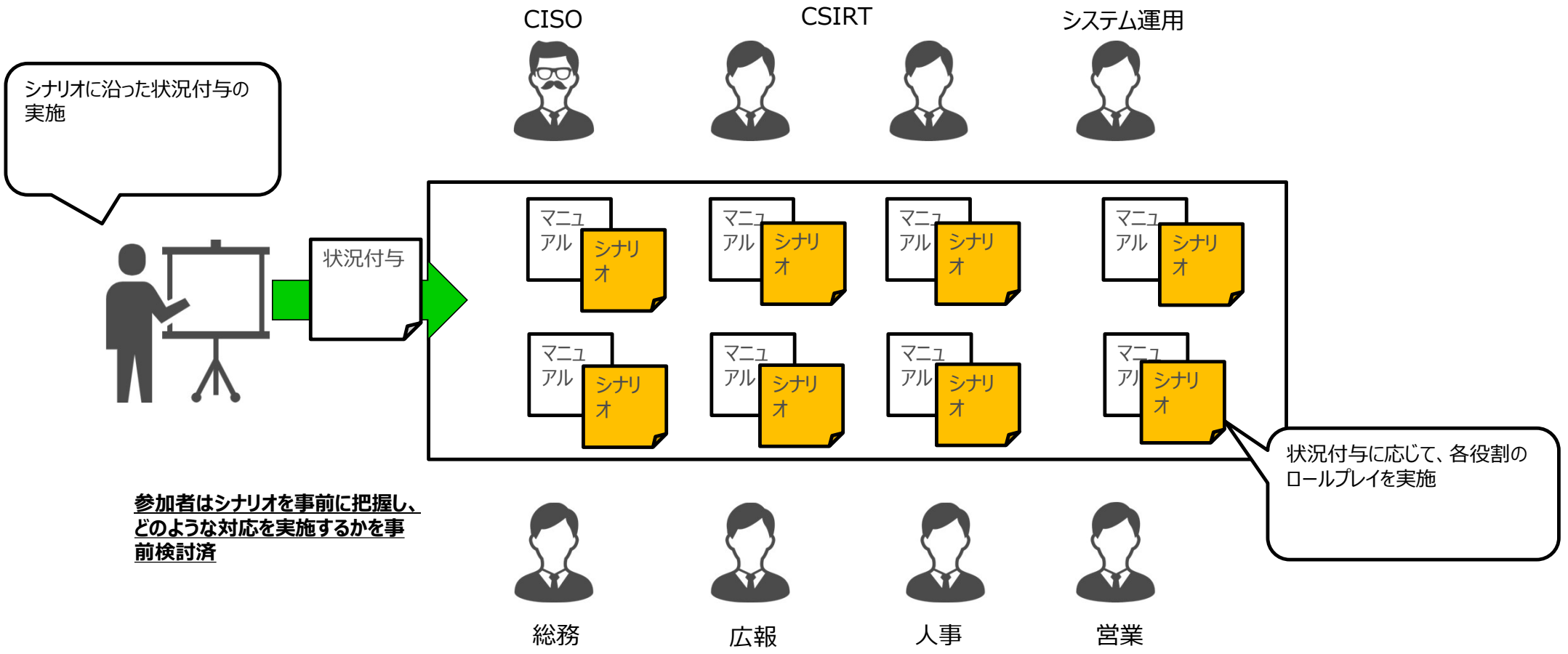
サイバー攻撃演習/訓練マップ③机上演習：シナリオ非開示型　イメージ



サイバー攻撃演習/訓練マップ④机上演習：シナリオ開示型

項目	内容
概要	• 参加者とファシリテータは会議室/リモート会議ツールにて集合して実施 • ファシリテータによる状況付与によって演習を実施。演習は主に会話によるコミュニケーションで実施 • シナリオを事前に開示。参加者はシナリオや状況付与を認識したうえで演習を実施
想定参加者	• CSIRT • インシデント対応関連組織　etc
演習実施環境	• 会議室/リモート会議ツール
効果	• インシデント対応フローの習得 • インシデント対応フローの課題洗い出し
難易度	★★★
備考	• シナリオを事前に参加者に開示することにより、参加者は事前に何を行うべきかを検討できる。インシデント対応力が未熟な参加者であっても、机上演習を円滑に実施できる

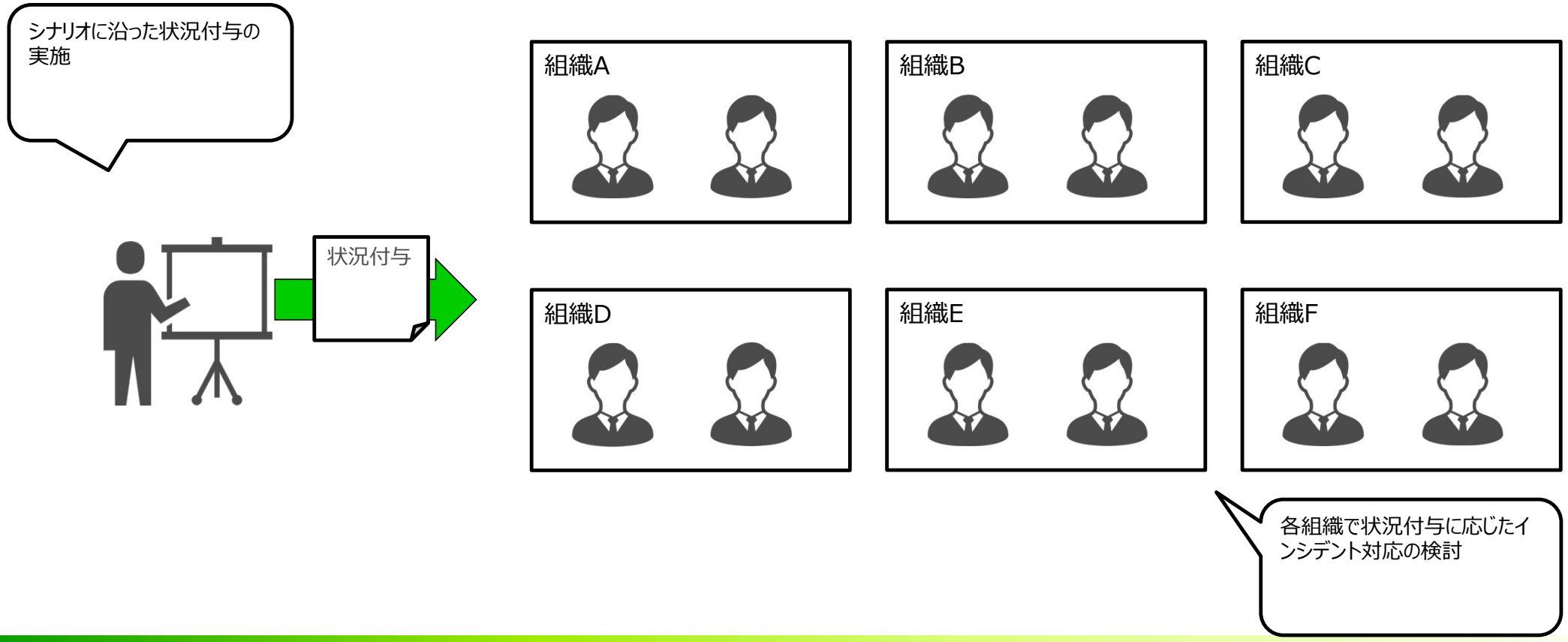
サイバー攻撃演習/訓練マップ④机上演習：シナリオ開示型　イメージ



サイバー攻撃演習/訓練マップ⑤机上演習：合同演習

項目	内容
概要	• 大企業のホールディングスCSIRT等が関連子会社をまとめて実施する演習 • 複数の組織が同様のシナリオで一斉に演習を実施 • 複数組織の演習を同時並行的に進めるため、事前設定した時間で、状況付与を続々と参加者へ提示していく • 状況付与により、参加者は組織ごとにディスカッションを行い、インシデント対応のアクションを決定する • シナリオは非開示
想定参加者	• 複数組織のインシデント対応に必要なメンバ
演習実施環境	• 会議室/リモート会議ツール
効果	• 複数の組織全体のインシデント対応能力の引き上げ • 組織毎のインシデント対応能力の確認、課題洗い出し • 組織毎へのインシデント対応の必要性の理解促進
難易度	★★★
備考	• 複数組織が対応可能なシナリオを作成する必要がある ・共通的な理解が可能なシナリオの作成 ・ベースのシナリオから、個別の組織ごとにカスタマイズを実施　etc

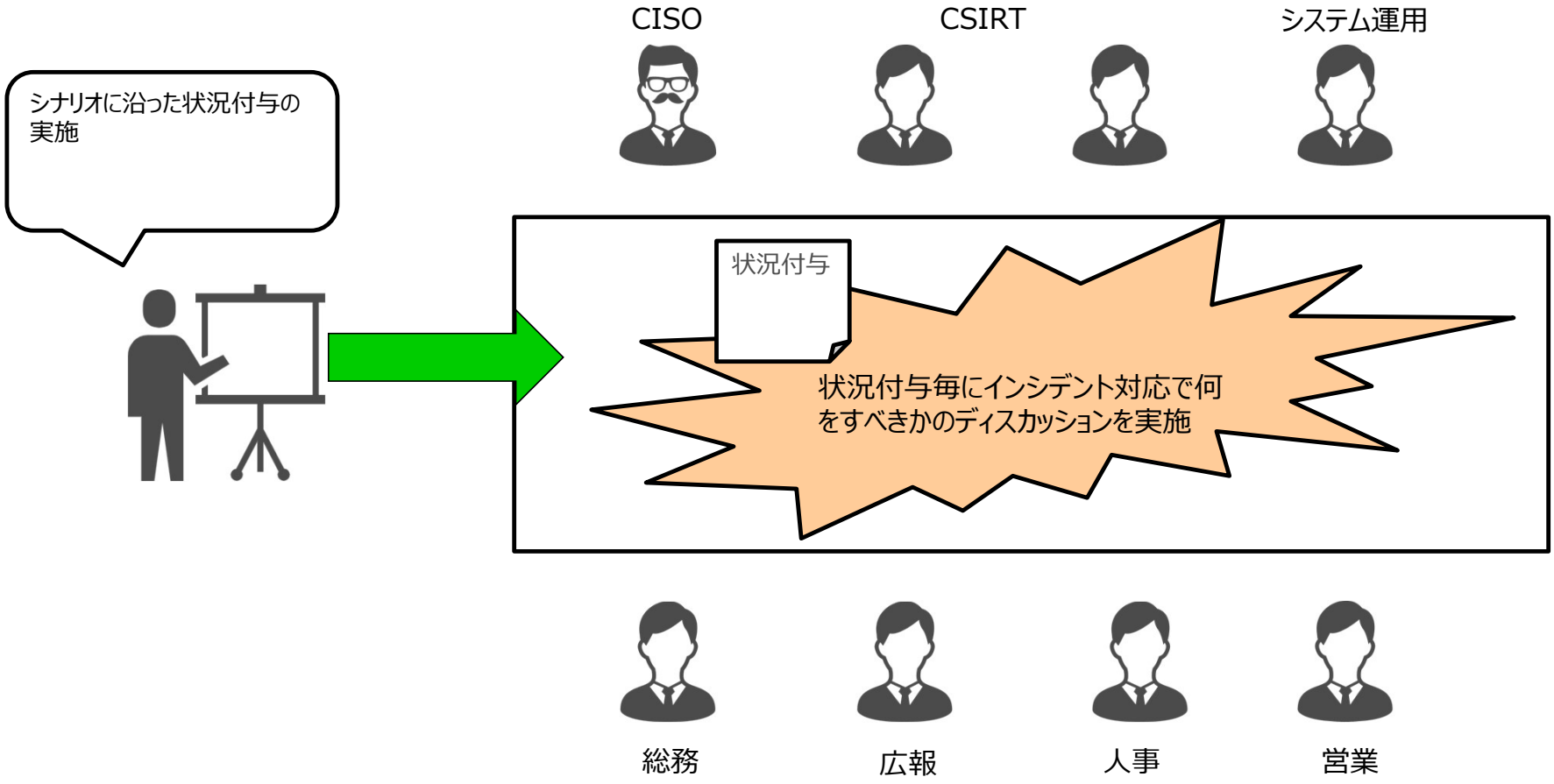
サイバー攻撃演習/訓練マップ⑤机上演習：合同演習　イメージ



サイバー攻撃演習/訓練マップ⑥机上演習：ディスカッション型

項目	内容
概要	• 参加者とファシリテータは会議室/リモート会議ツールにて集合して実施 • ファシリテーターによる状況付与を提示。 • 参加者はファシリテータより提示された状況付与に応じた、インシデント対応に関するディスカッションを実施 • シナリオは非開示
想定参加者	• 複数組織のインシデント対応に必要なメンバ
演習実施環境	• 会議室/リモート会議ツール
効果	• インシデント対応フローの理解 • インシデント対応フローの課題洗い出し • インシデント対応フローに記載がないような事象に関する検討力の向上
難易度	★★★
備考	• インシデント対応やロールプレイに不慣れな参加者の場合、ロールプレイの実施が困難である場合がある。個々の状況付与に個別にディスカッションを実施することにより、演習の効果を得ることが可能である。

サイバー攻撃演習/訓練マップ⑥机上演習：ディスカッション型　イメージ

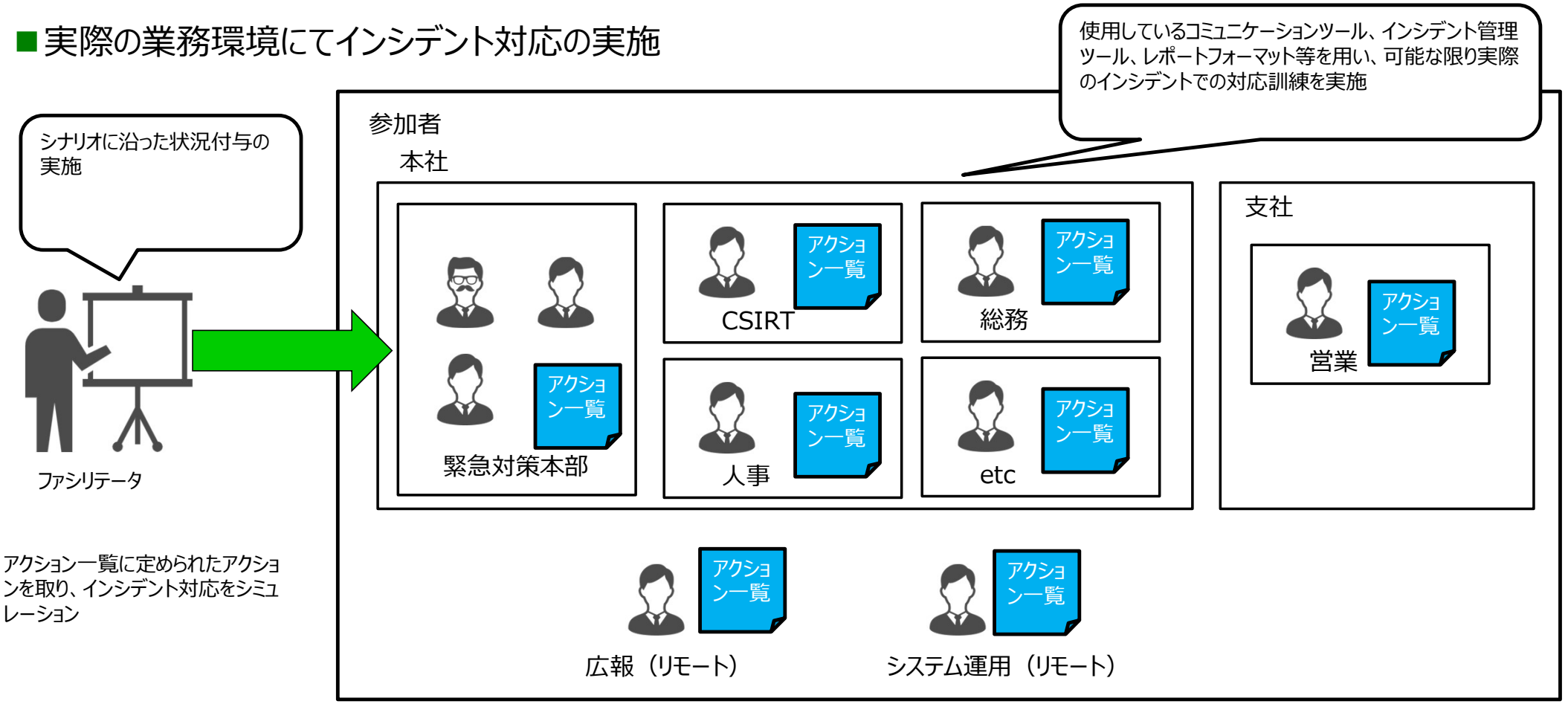


サイバー攻撃演習/訓練マップ⑦机上訓練：実環境型

項目	内容
概要	• シナリオや参加者の想定するアクションは全て定義されている。参加者は定義されたシナリオ通りの行動を実施する。 • 参加者は、実際に組織で用いるインシデント対応時に利用するコミュニケーションツール(電話、メール、チャット、リモート会議ツール、インシデント管理ツールetc)を用いて訓練を実施
訓練実施環境	• 参加者の業務環境
効果	• インシデント対応フローの理解促進 • インシデント対応時のコミュニケーションツールの把握 • 訓練の実施実績。机上演習実施に向けてのステップアップ • 定型のフローやルールの確認
難易度	★★
備考	• 参加者のアクションをすべて定める必要があり、シナリオ作成に相当時間を要する • 参加者は事前知識なしでもインシデント対応の訓練が実施可能である

サイバー攻撃演習/訓練マップ⑦机上訓練：実環境型　イメージ

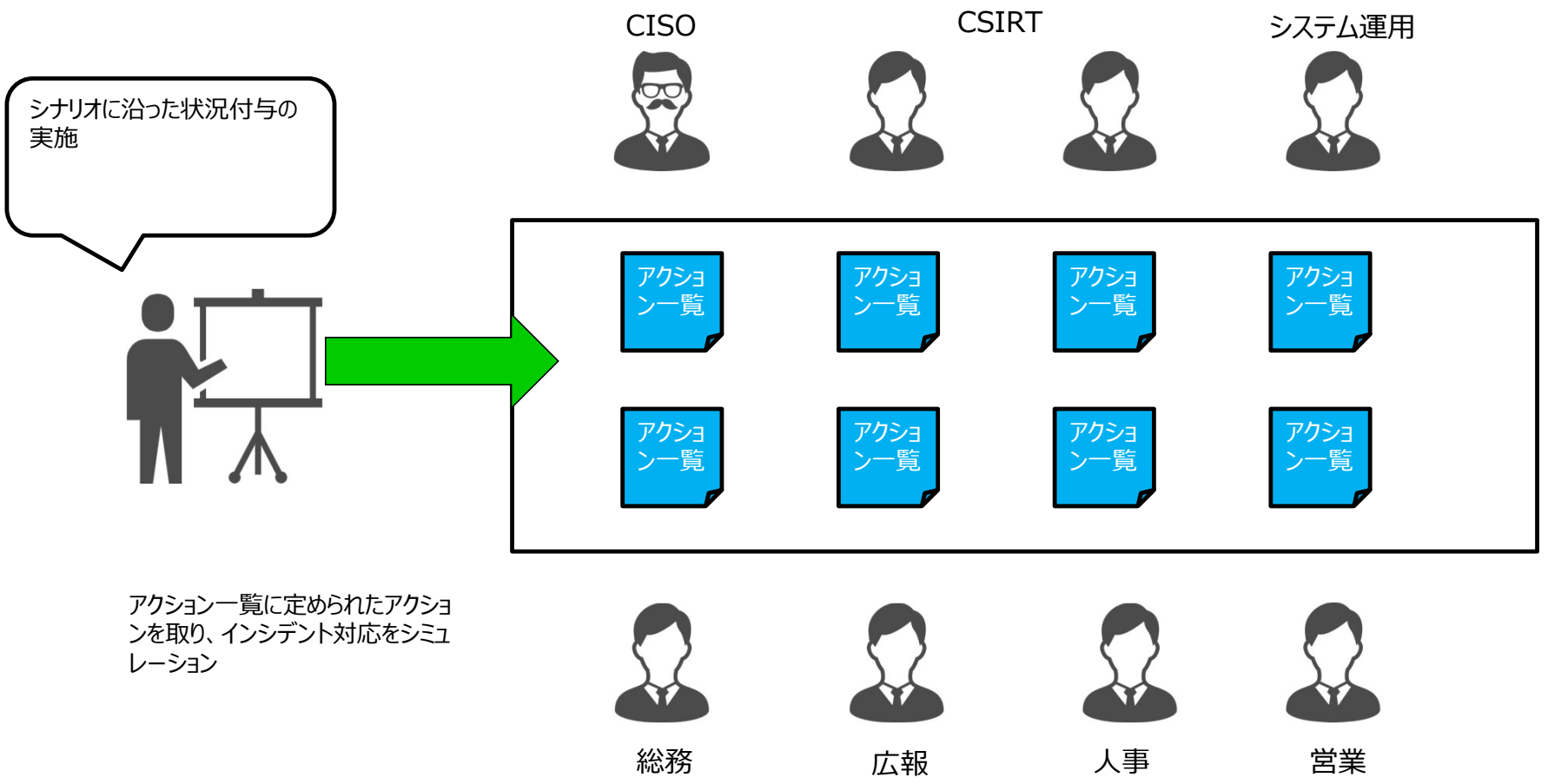
■実際の業務環境にてインシデント対応の実施



サイバー攻撃演習/訓練マップ⑧机上訓練：集合型

項目	内容
概要	• シナリオや参加者の想定するアクションは全て定義されている。参加者は定義されたシナリオ通りの行動を実施する。 • 参加者は、会議室/リモート会議ツールで集合して訓練を実施する。訓練は主に会話によるコミュニケーションで実施
訓練実施環境	• 会議室/リモート会議ツール
効果	• インシデント対応フローの理解促進 • インシデント対応時のコミュニケーションツールの把握 • 訓練の実施実績。机上演習実施に向けてのステップアップ • 定型のフローやルールの確認
難易度	★★
備考	• 参加者のアクションをすべて定める必要があり、シナリオ作成に相当時間を要する • 参加者は事前知識なしでもインシデント対応の訓練が実施可能である • 集合形式で実施により、実環境型より円滑に訓練の実施が可能

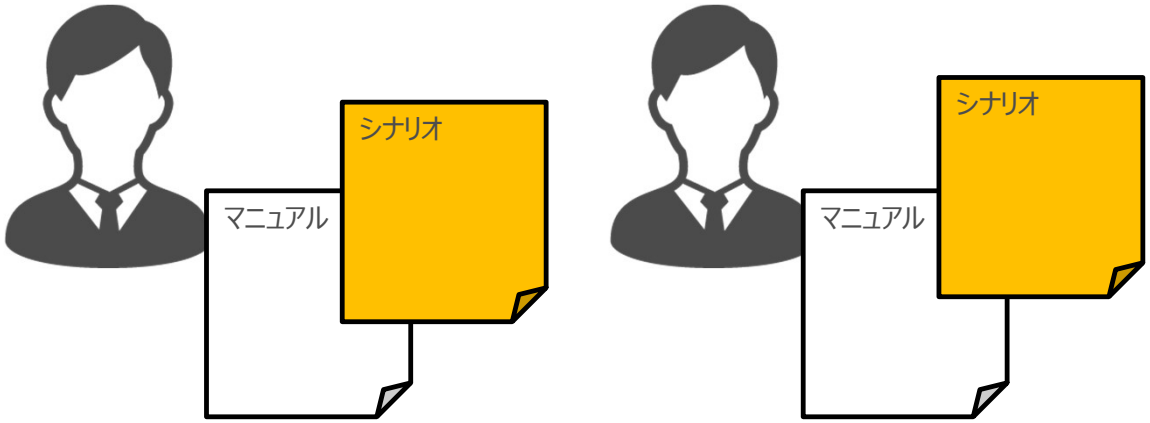
サイバー攻撃演習/訓練マップ⑧机上訓練：集合型 イメージ



サイバー攻撃演習/訓練マップ⑨机上訓練：ウォークスルー型

項目	内容
概要	• シナリオをベースとしてとして、既存のインシデント対応フローの読み合わせを実施する
訓練実施環境	• 会議室/リモート会議ツール
効果	• インシデント対応フローの理解促進 • インシデント対応フローの課題の洗い出し • 定型のフローやルールの確認
難易度	★
備考	

サイバー攻撃演習/訓練マップ⑨机上訓練：ウォークスルー型イメージ



インシデントシナリオをベースとして、インシデント対応フロー等の読み合わせを実施

執筆および協力者一覧

■石塚　元	専門委員
■阿野 勝	TOMARI-CSIRT
■井出　雄介	PIRATES
■伊藤 圭亮	IL-CSIRT
■加藤　孝浩	ToppanForms-CERT
■今 佑輔	TM-SIRT
■篠 知佐	KCCS-CSIRT
■羽場 満	Canon-CSIRT
■増田 佳弘	SHIFSIRT
■渡辺 文恵	DeNA CERT

改訂履歴

- 2021年12月21日 Ver. 1.0　作成
- 2022年04月18日 Ver. 1.1　改訂
- 2022年05月10日 Ver. 1.2　「執筆および協力者一覧」修正
- 2023年03月20日 Ver. 1.3　外部公開版