サイバー攻撃対応演習の意義 ～Telecom-ISAC Japan サイバー攻撃演習2009の実施結果から～

Telecom-ISAC Japan
サイバー攻撃演習ワーキンググループ主査
則包　真一

はじめに

セキュリティの話しを聞きに来られている方々にいきなり演習の話しを訥々としても、、と思いますので、まずはウォーミングアップから。

訓練も演習の一種ですが、一番身近ものとして防災避難訓練があります。

避難訓練の意義/目的（何を実施できることを意図して実施しているか）を３点～５点位挙げてください。（検討時間3分）

-
-
-
-
-

避難訓練の意義

参加者のスキル確認/向上
・館内放送をしっかり聞いて、情報入手し判断できるようにする
・消防署等への的確な状況通報ができるようにする

判断の訓練である
「ビルの何階の何処で火災が発生」から避難経路の選択、誘導班の指示に従い避難、等々与えられる情報により判断する

・避難の経路を確認/理解する
・避難場所を確認/理解する
・火災のときには口にハンカチをあてる等適切な対応を行えるようにする
・誘導班等の役割ができるようにする
・全員の避難ができたか確認できるようにする

行動の訓練である
自分で対応すること、どのように対応/行動したらよいかを訓練する

想定外の把握
・館内放送がわかりずらかった
・避難出口に人が集中して大変だった
・ハイヒールだと階段を降りるのが困難だった
・全員が避難できたのか確認できなかった
・避難に時間がかかり過ぎた

課題抽出の機会である
想定していなかったこと、抜け落ちていたことを確認する

別の視点から

数年前のあまりメジャーな映画ではなかったのですが、ある映画の中で、主人公のニコラス・ケイジ演じる詐欺師が、弟子にしてくれとせがむ実の娘に、次のことを語っています。

「どんなに入念な計画を立てていても、必ず、想定外の危機は起こるものだ。詐欺を成功させるには、危機に遭遇したとき、いかに上手く対処するかがポイントだ」

これは詐欺を成功させるための秘訣として語った一言です。

↓ 世渡りの達人の言葉ですが、一般的サービス運用に置き換えると

「どんなに入念な計画を立てていても、想定外のインシデントは必ず起こるもの。
安定したサービス提供を成功させるには、インシデントに遭遇したとき、いかにうまく対応できるかがポイントである」

想定外の危機に対応するためには

一次判断
対応すべき危機（インシデント）であるか判断する

初動が大切。重要なインシデントを認識せずに後から取り返しのつかないことになったり、大したインシデントでないのに過剰に反応したりする。

二次判断
自分で対応できることは何か、どのような対応をしたらよいかを決める。

↓

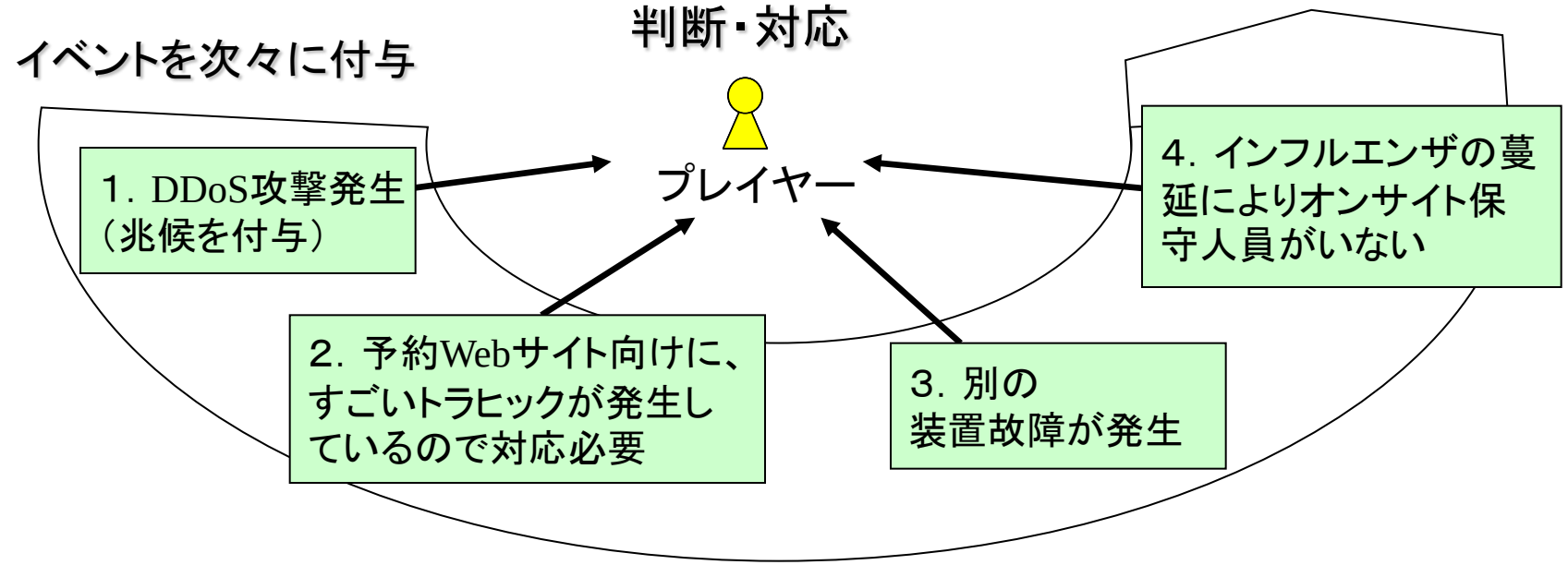
一次判断（危機かどうかの判断）と二次判断（何をしたらよいかの判断）がうまくできれば、危機（インシデント）への道筋はできたと考えてよいです。

だが、危機（インシデント）を体験するチャンスは通常業務では限られます。逆に、毎日危機が発生していたら大変です。

想定外の危機に対応するためには

どれだけ体験しているかが肝です。平時には体験できません。
演習により擬似体験、シミュレーションができます。

重要サイト運用者向け演習例：



いろいろなインシデントが発生するシナリオを作成し、一次判断の訓練をします。そのときに自分で出来ること/対応すべきこと（二次判断）の訓練もできます。さらに、組織として、対応時に抜け落ちている事項を抽出できます。

このお話しの後どのようになっていただきたいか

第一段階：　演習に興味を持つ、必要であることを理解する

第二段階：　演習に参加してみたいと思う

第三段階：　演習を企画、実施してみたいと思う

全体構成

第一章　演習実施の意義

　　演習って何で必要であるかについて説明しました

第二章　実際の演習の様子

　　昨年末に実施した演習について紹介しつつ、演習について説明します。（演習がどんな感じで行われるか理解してもらいたいと思います。）

第三章　演習の作り方

　　演習を実際に実施する場合にどのように設計して実施していくのか、注意点等を説明します

第二章　実際の演習の様子

2009年度サイバー攻撃対応演習

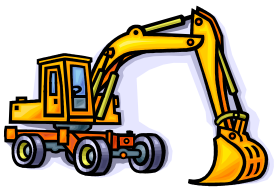
昨年12月11日（金）
朝9時から夕方5時すぎまで、
大田区産業プラザにて開催

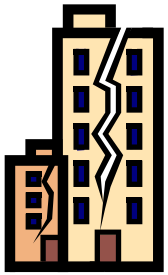
参加者
・重要インフラ→ネット証券会社、ロジスティックス会社　合計3社
・電気通信事業者→国内主要ISP、アクセス網事業者　合計8社
・政府関係者、テレコムアイザック　等
総勢100名強が参加

サイバー攻撃対応演習の対象は

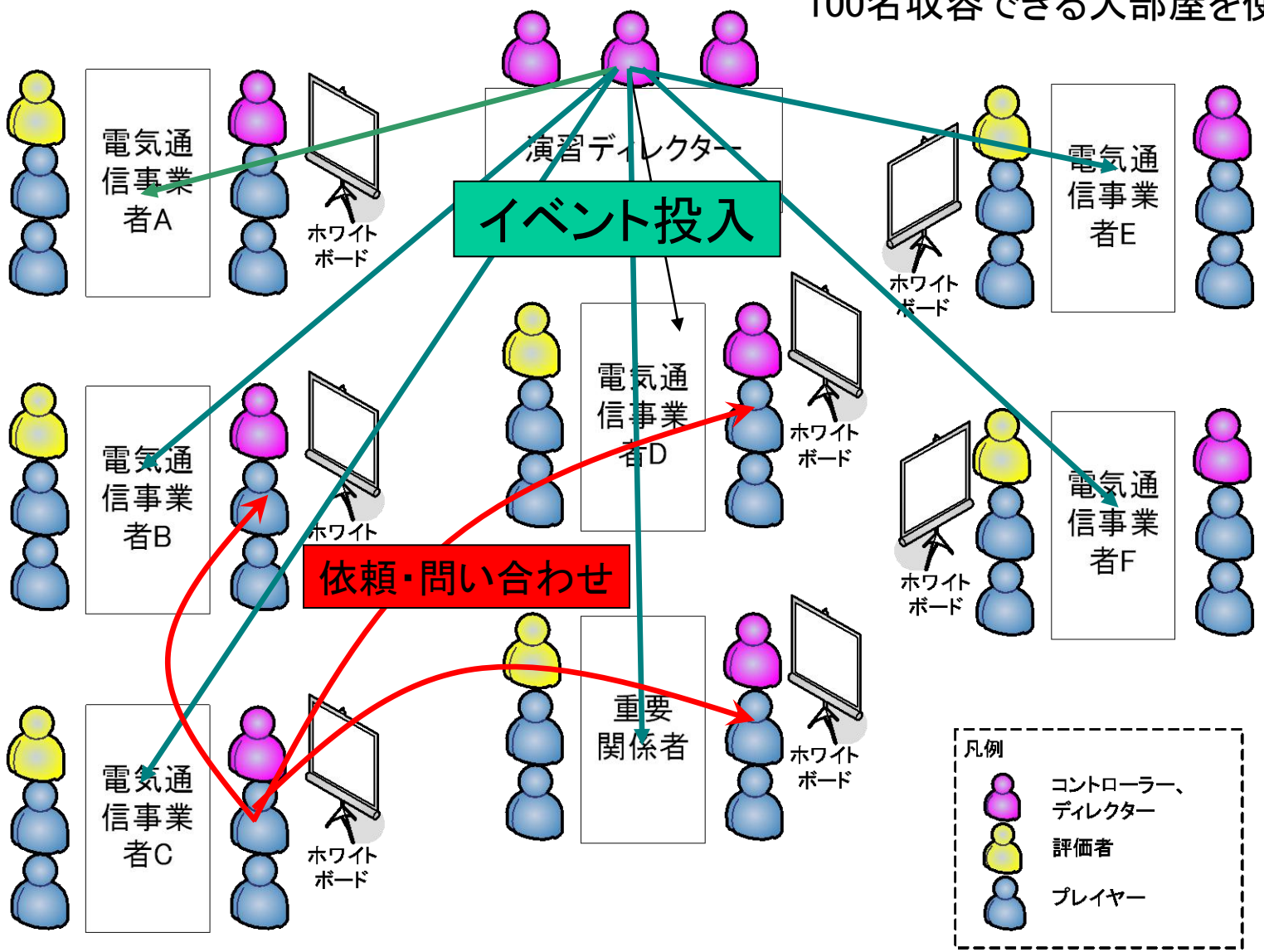
IT通信インフラの障害という特定の緊急事態を念頭に設計された危機管理演習です。人的過失、自然災害、あるいはハッカー、犯罪者、テロリストまたは他国政府からの攻撃によって発生する障害を想定します。

つまり、ハッカーとかBotによる攻撃のみを想定するものではなくIT通信インフラ障害を引き起こすもの全てを対象とします。





サイバー攻撃対応演習の進め方



対応の様子

動画で各島での議論の様子とディレクター、コントローラー、
プレイヤーの役割を少々紹介します

演習の進め方

①大会場に集合。進め方を説明

②ディレクターがイベントを投入

③参加者島毎に対応を検討・他島問合せ

演習のメインです。プレイヤーの訓練を実施し、各社で課題を抽出します

④島毎にコメント発表、全体講評

連携等の各社共通的課題や自社における改善点等を中心に発表します

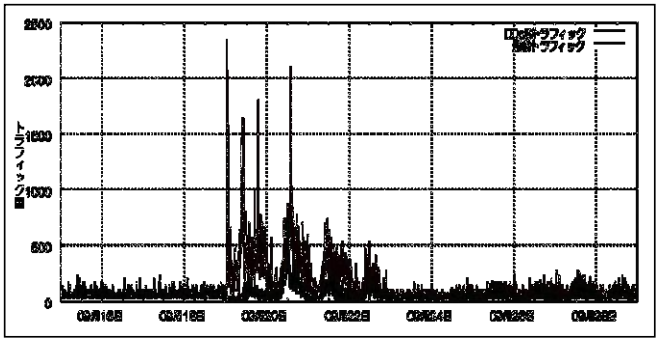
投入イベントとプレイヤーの対応（DDoSでの例）

投入イベント

演習では、文章、数字、図、グラフなどで情報をプレイヤーに付与する

プレイヤーの（想定）対応

第一イベント



→ DDOS検知
急激なトラヒック増DDoS攻撃ではないか

第二イベント

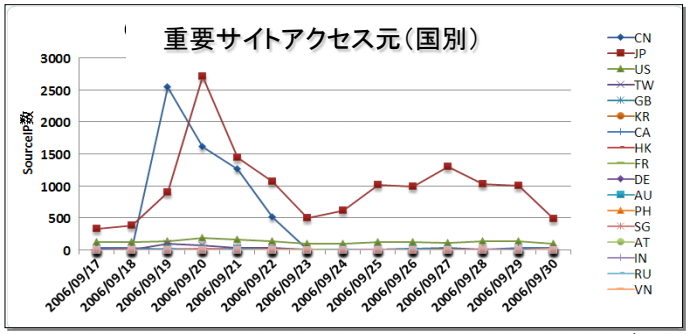
重要ユーザから
予約受付Webサーバ
CPU/メモリ使用率100%
Webサイト接続が不可能との苦情が多数来ている
なんとか対応お願いしたい

→ 重要ユーザがDDoS攻撃により、被害を受けている。
重要顧客であるうえに、社会的に止まると影響度の大きいサイトである。
なんとか対応しなければ。。

イベントへのプレイヤーの対応（DDoSでの例）

投入イベント

第三イベント



CN国からのアクセスが急増していることがわかる

第四イベント

国内ISPからの重要インフラ宛の通信も急増してきた。自社のルータのフィルターでは負荷が高く対応し切れない。

プレイヤーの（想定）対応

CN国との境界ルータにて、トラヒックを制御しよう。
重要サイト向けのパケットを選択して破棄する設定をしよう。

主要なピア先のISPに重要サイト向けのトラヒックのフィルターをお願いしよう。

イベントへのプレイヤーの対応（DDoSでの例）

投入イベント	プレイヤーの（想定）対応
第五イベント	
DDoS攻撃は特定ポートを使用したものであることがわかった。	重要インフラ向けの特定ポートの通信をフィルターしてしまおう。
第六イベント	
DDoS攻撃が収まる	・とりあえず対応終了。 ・当面フィルターの設定等は様子を見て継続しておこう。 ・再発時の対応を検討しておこう。

注意：
ここで記述したやりとりは演習上の仮定です。
全ての電気通信事業者がここまで対応することを保障するものではありません。

演習で実施された攻撃

・DDoS（サービス不能攻撃）

一般のインターネットユーザを受け入れているサイト等は攻撃自体とめる方法がない。攻撃を止めるとサービスの提供も止まってしまう。

・BGP経路ハイジャック

よく発生するのは、ミスオペ。
検知する方法はいろいろ工夫（経路奉行など）
現在では、完全に止める方法はない。

・DNSサーバ関連の攻撃

DNSプログラムの脆弱性は適宜発見され、その脆弱性を利用した攻撃が発生する可能性がある。
DNSが止まってしまうとインターネットへの影響が甚大である。

・その他

悪性サイトへのアクセスなど

参加者の声（「参加者アンケート」から）

分類	参加者の声
個人の役割上での意見 （対応すべきインシデントの判断、対応方法）	・机上の演習ではあったが、事の発生から経過を経験できてよい ・担当者の個人差を埋めるために演習で経験を積ませるのは有効である ・いざというときに役立ちそうである ・例年参加しているプレイヤーは演習慣れしている。実際のアタックの際に落ち着いて対応する必要性を考えると効果が出ているといえる ・初参加の若手プレイヤーからも好評であった
組織としての機能に関する意見 （組織としてインシデント対応で抜け落ちていた機能等）	・大枠で対応ポリシーが決まっていたが、実行レベルでは十分ではないことがわかった ・社内向けの連絡先は整備/周知されていたが社外の連絡先が未整備であった ・専門知識を有した担当者の判断が必要な場合に不在時に対応する体制がないことがわかった ・発生頻度の高い既知のインシデントについては社内対応フロー上問題はないが、未知のインシデントについては担当の経験により実行レベルに差がでることがわかった

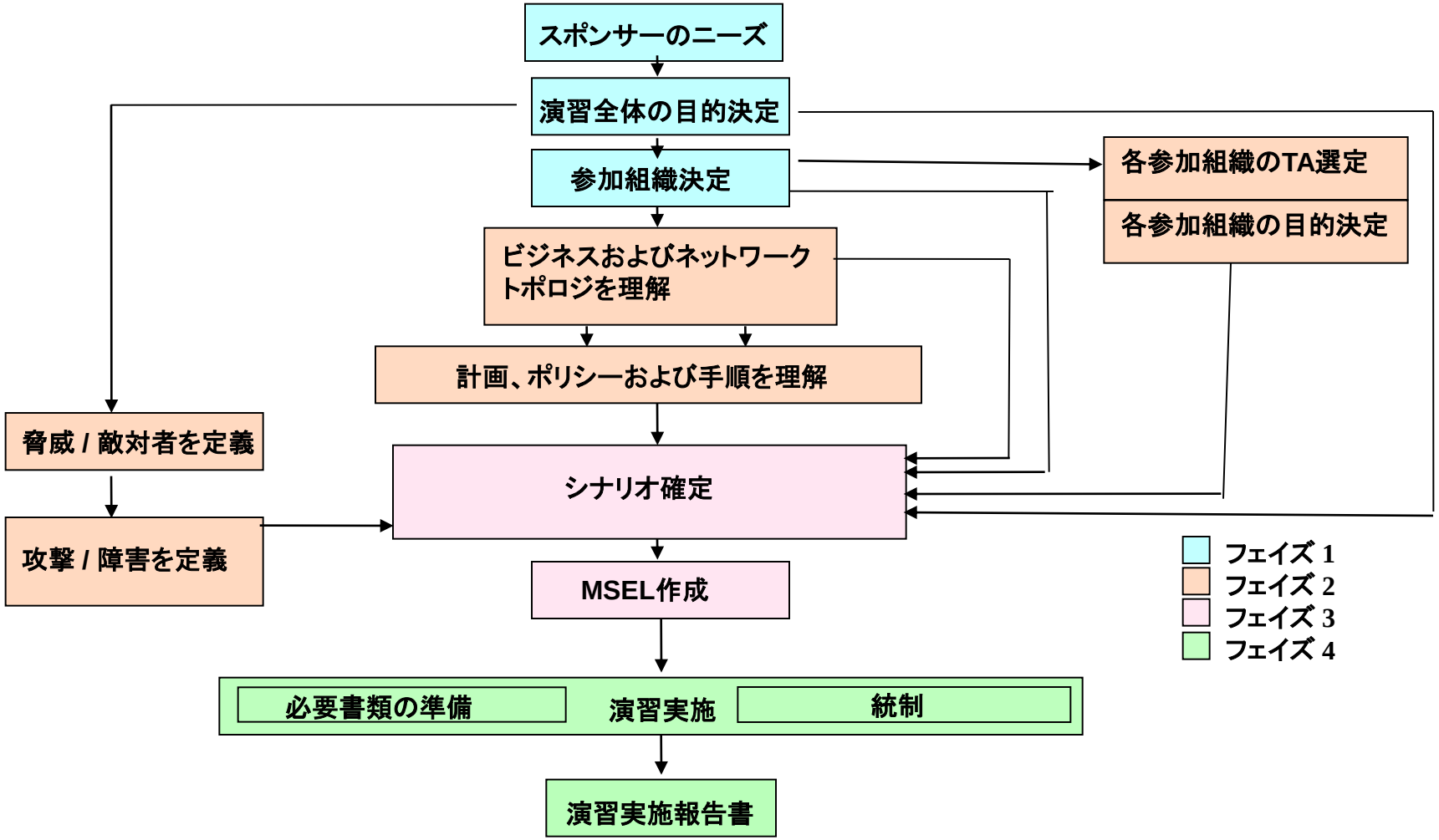
参加者の声分析

プレイヤー
・演習参加当初のモチベーション水準によらず、演習に参加した人はその効果を実感し、来年度も参加したいという意見がほとんど
～対応訓練（ドリル）としての意義を感じてもらっている

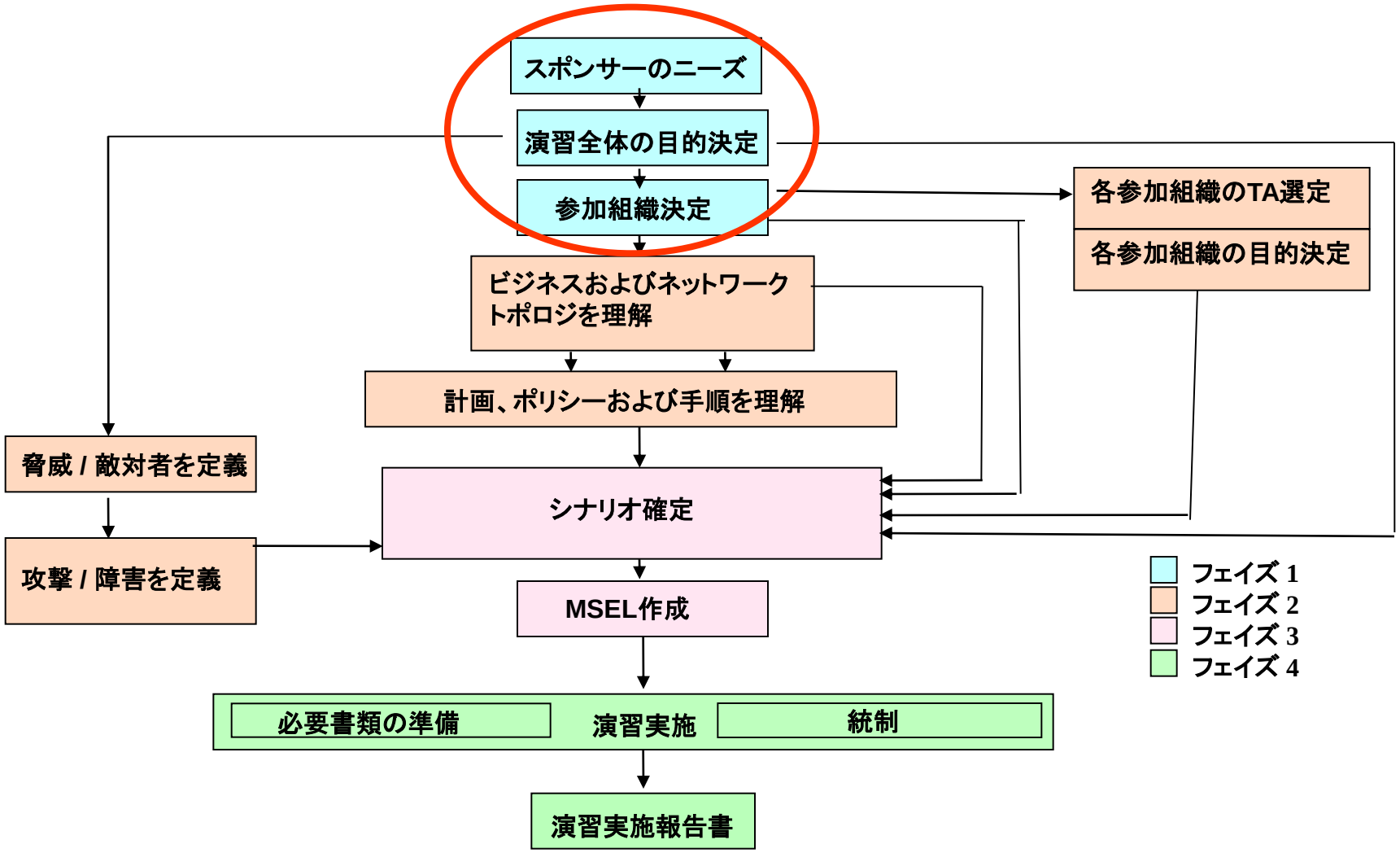
課題抽出
・何年か参加している企業であっても、演習により新たな課題が抽出されている。
～対応環境や攻撃の変化により、業務運用のチェックが定期的に必要であることがわかる。

第三章　演習の作り方

シナリオの作り方



下図の　話しをします



スポンサーニーズ、全体目的の決定

スポンサーのニーズ
↓
演習全体の目的決定

スポンサーって誰？
→お金を出してくれる人（業界団体、政府等）、やれと命令した人（社長、運用責任者等）

次のステップで進める
- **ヒアリング等を実施し、スポンサーのニーズを理解し整理し文書化する。**
- **ニーズについてスポンサーと合意する。**
- **ニーズに応じて演習全体の目的を設定する。**

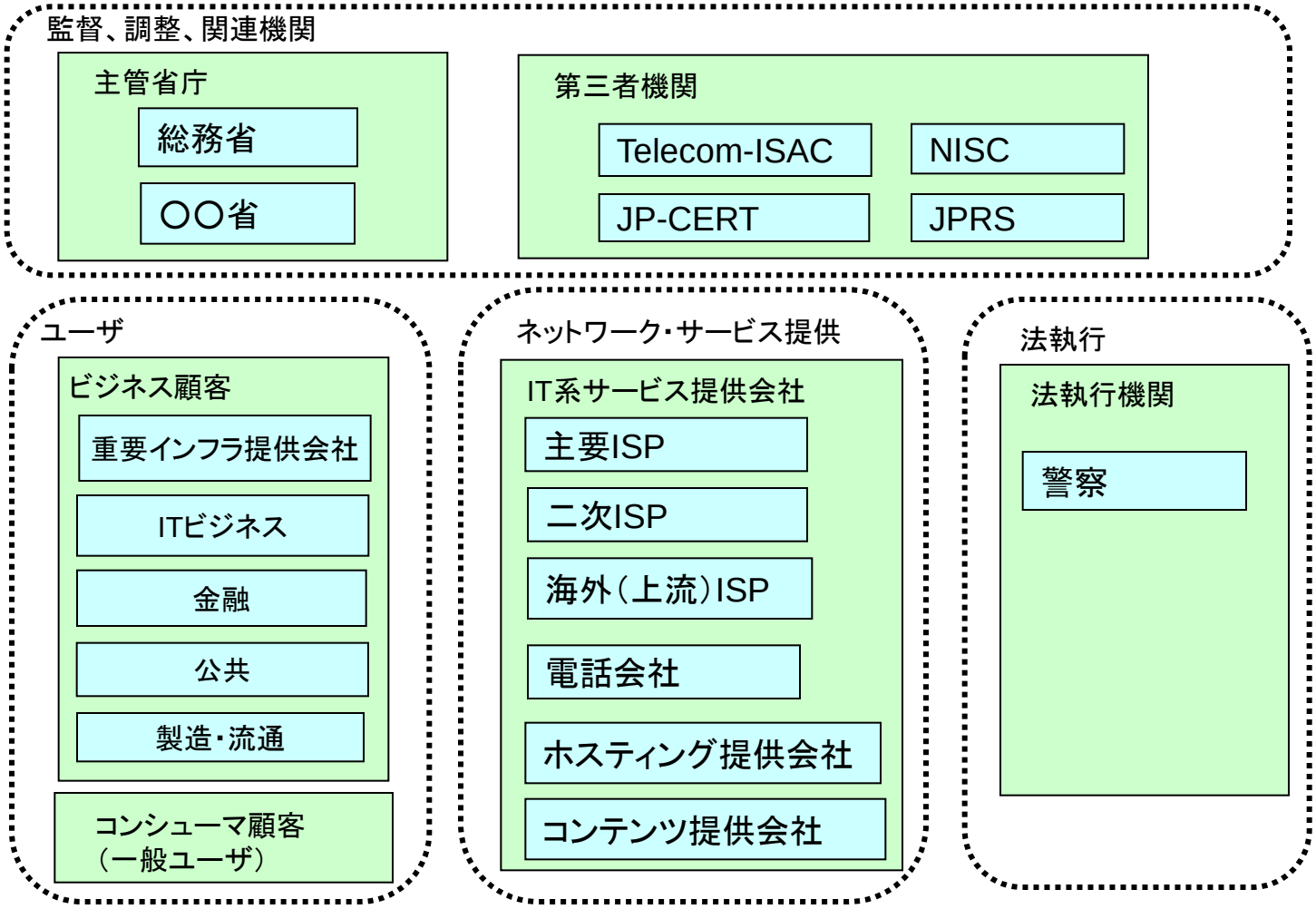
サイバー攻撃対応演習の場合	
スポンサーのニーズ	社会インフラとして、サイバー攻撃があっても安心して安全に使えるインターネットの実現
演習全体の目的	・サイバー攻撃により社会インフラに重大な影響が発生した場合、特に電気通信事業者単独では解決できない事例や事項に対して、速やかに**電気通信事業者間で横断的な連携**を行い事象解決するための課題を抽出し、その対策強化を実現すること ・サイバー攻撃に対応できる高度なITスキル・調整力をもった**人材を育成する**こと

参加組織の決定

参加組織決定

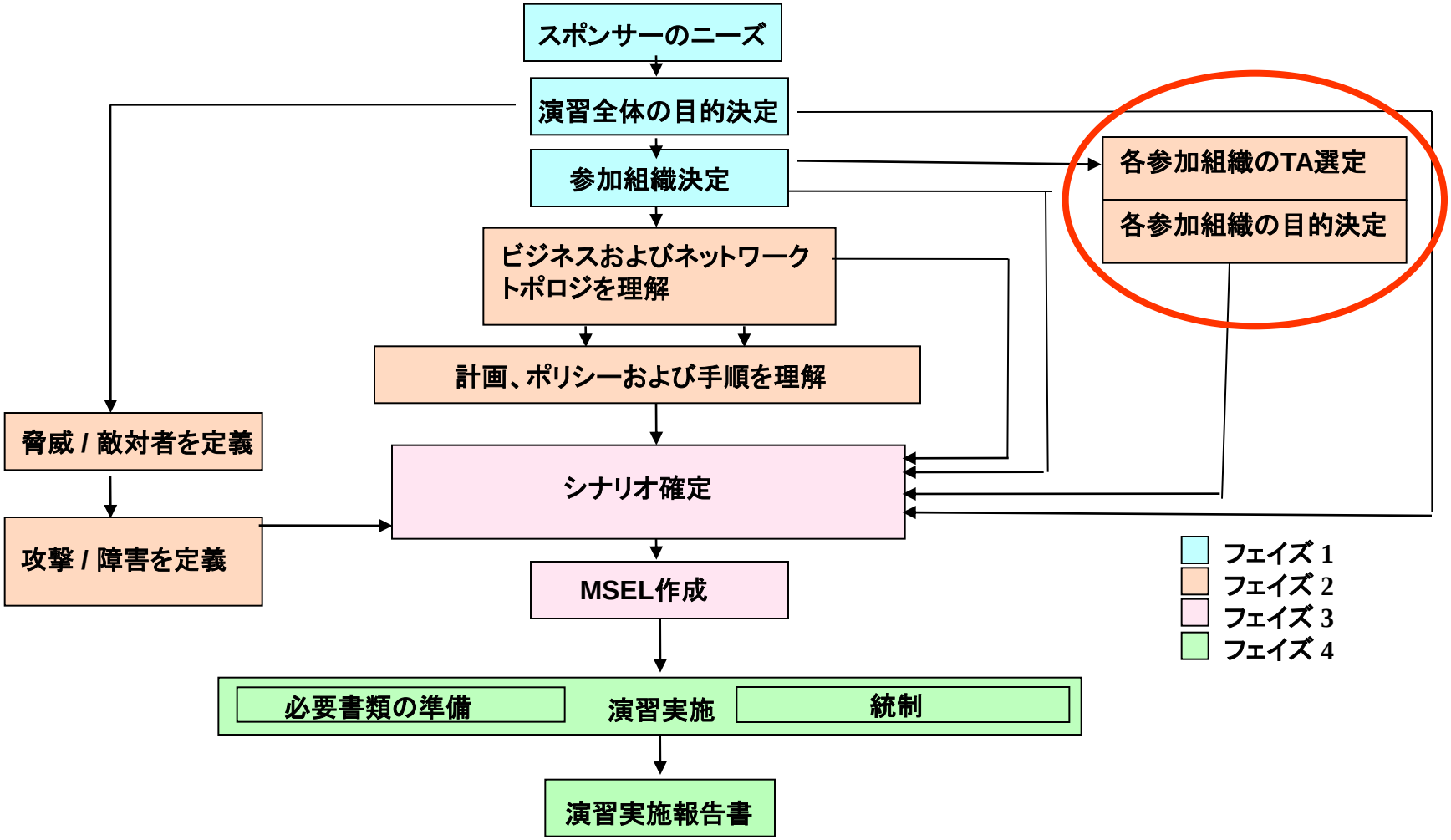
・演習目的達成に必要な組織を選定する。
・参加の確約を取り付ける。

サイバー演習で想定した組織例



・参加が困難な組織に関しては、SimCellとして設定し、有事の際の対応を想定した擬似の対応者で代替することができる。

下図の ○ 部分の話しをします



各参加組織のTAを選定

演習を成功させるために特に重要！！

TA（Trusted Agent）とは

　演習参加組織の代表です。シナリオ設計者に対してとして攻撃を受ける側の情報を提供します。

　自社の参加目的や業務ポリシー・手順、ビジネス環境・ネットワーク環境などの情報をシナリオ設計者に提供し、演習シナリオ設計をサポートします。

TAがいると痛いところをついた攻撃ができます。つまり、参加者の演習参加目的にあった、実効性のある演習が実施できます。

TAが考えておくべきこと

- 演習参加組織の代表者として、自社が演習に参加することのメリット・達成したいことなどを整理しておく
- どのような攻撃が仕掛けられた場合の演習を実施したいのか
- 攻撃による影響範囲はどこまでなのか
- 攻撃に対してどのような対応を実施するか

参加組織の目的決定

各参加組織の目的決定

演習を成功させるために特に重要！！

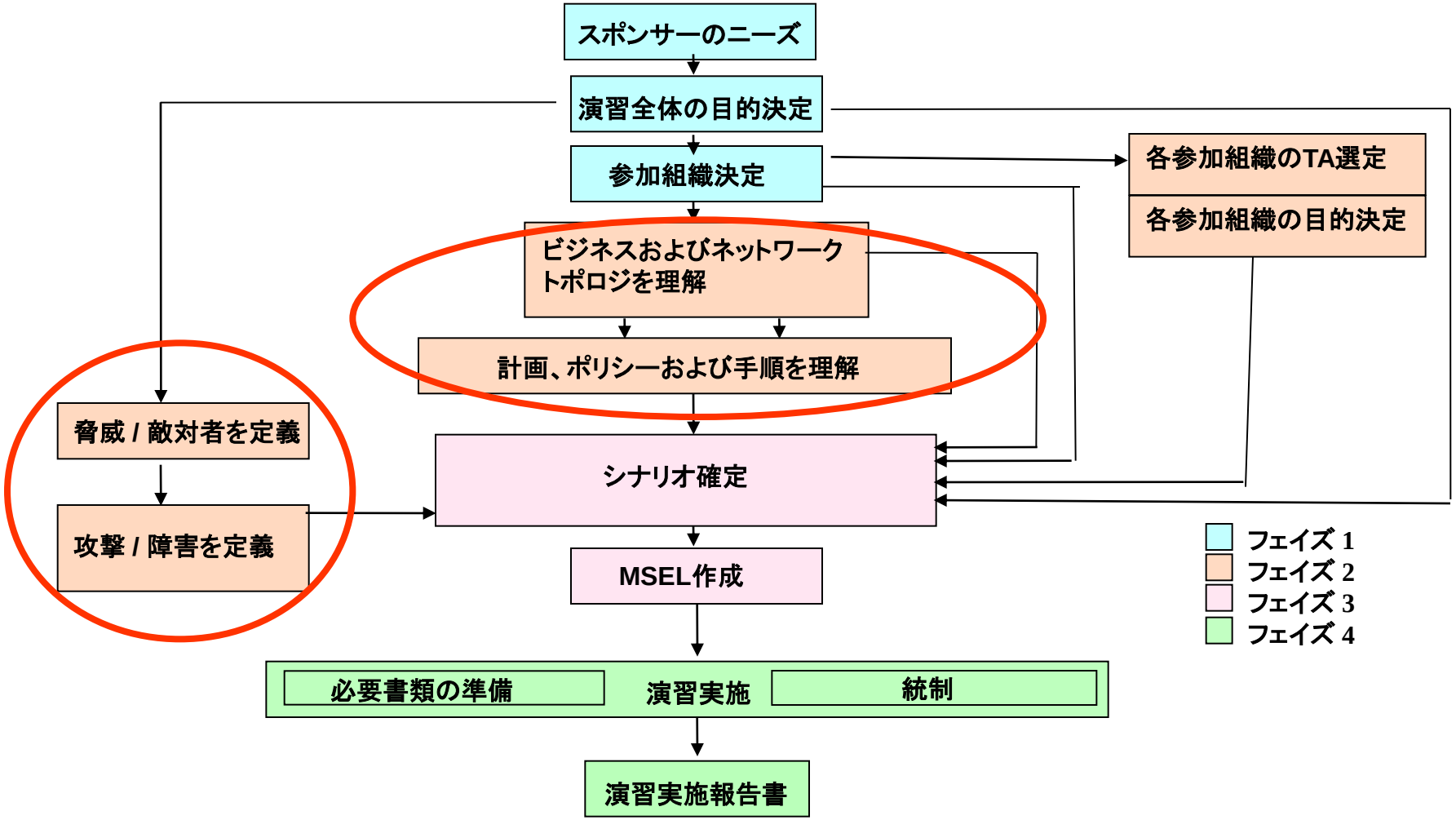
参加者の参加目的を十分に把握する

- よく把握していないとすぐに参加者に逃げられます

演習に興味を持って参加した人は特に、目的がずれてきて参加メリットがなくなると、すぐに脱落します。

逆にしがらみで参加している人は最後まで付き合ってくれるかもしれませんが、それはそれで問題です。

下図の ○ 部分の話しをします

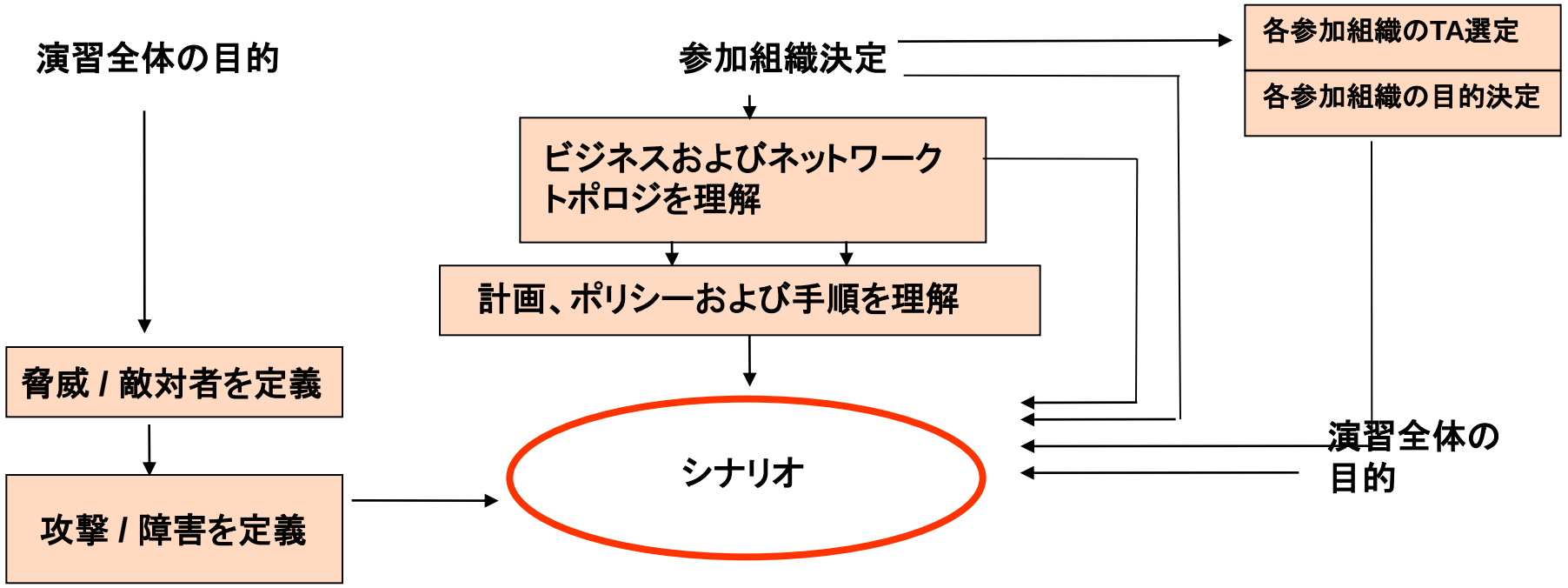


敵を知り、己を知る

演習を現実に即したものに！

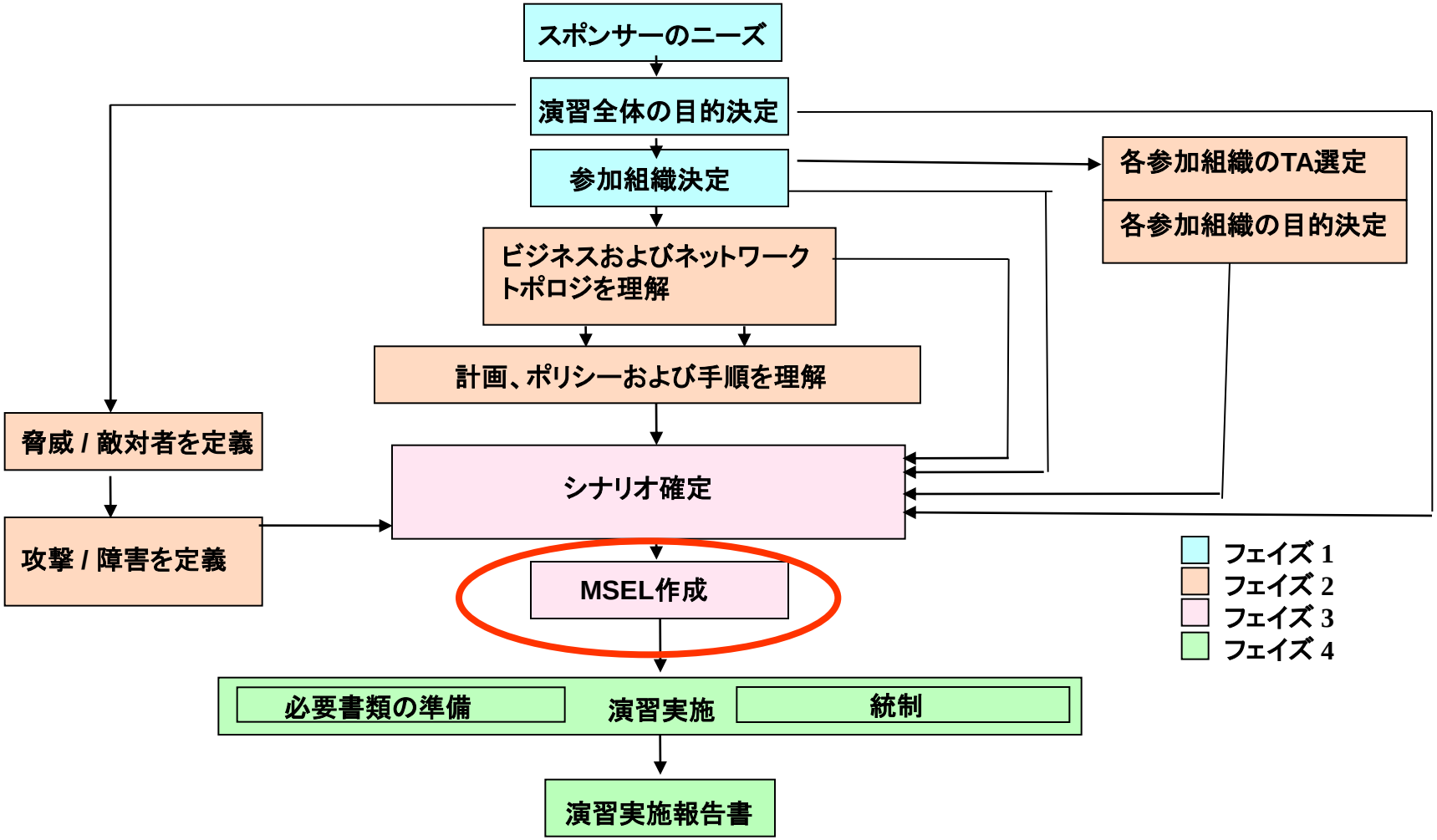
	項目	実施すること	例
己を知る （TAから収集）	ビジネス環境	止まるとビジネスに影響のあるシステムを抽出	個々のシステムの確認 ・取引企業間決済システム ・受発注システム ・社内システム（メール、給与、人管等）　等
	ネットワーク環境	システム間を接続するネットワークの現状を調査	ネットワーク関連規定類の確認 ・システム間連携図 ・業務フロー ・NW構成図、機器一覧 ・使用ソフトウェアバージョン情報　等
	攻撃への準備	攻撃に対しての対応方針、計画、手順を確認	運用関連規定類の確認 ・運用マニュアル（対応手順、回復手順含む） ・エスカレーション手順、不測事態対応計画 ・セキュリティポリシー、BCP　等
敵を知る （脅威設計者から収集）	脅威・攻撃	社会的背景をもとに、潜在的・顕在的な脅威・攻撃の洗い出し	攻撃対象と攻撃内容の確認 ・サーバへの攻撃 ・ネットワーク機器への攻撃　等

シナリオの作り方



- シナリオは参加者の目的を中心に構築し、目的を達成できなければならない
- シナリオはリアルなものでなければならない
- シナリオは疑問を持たれず納得されるものでなければならない
- 意思決定者にいかにダメージを与えるかも重要

下図の ○ 部分の話しをします



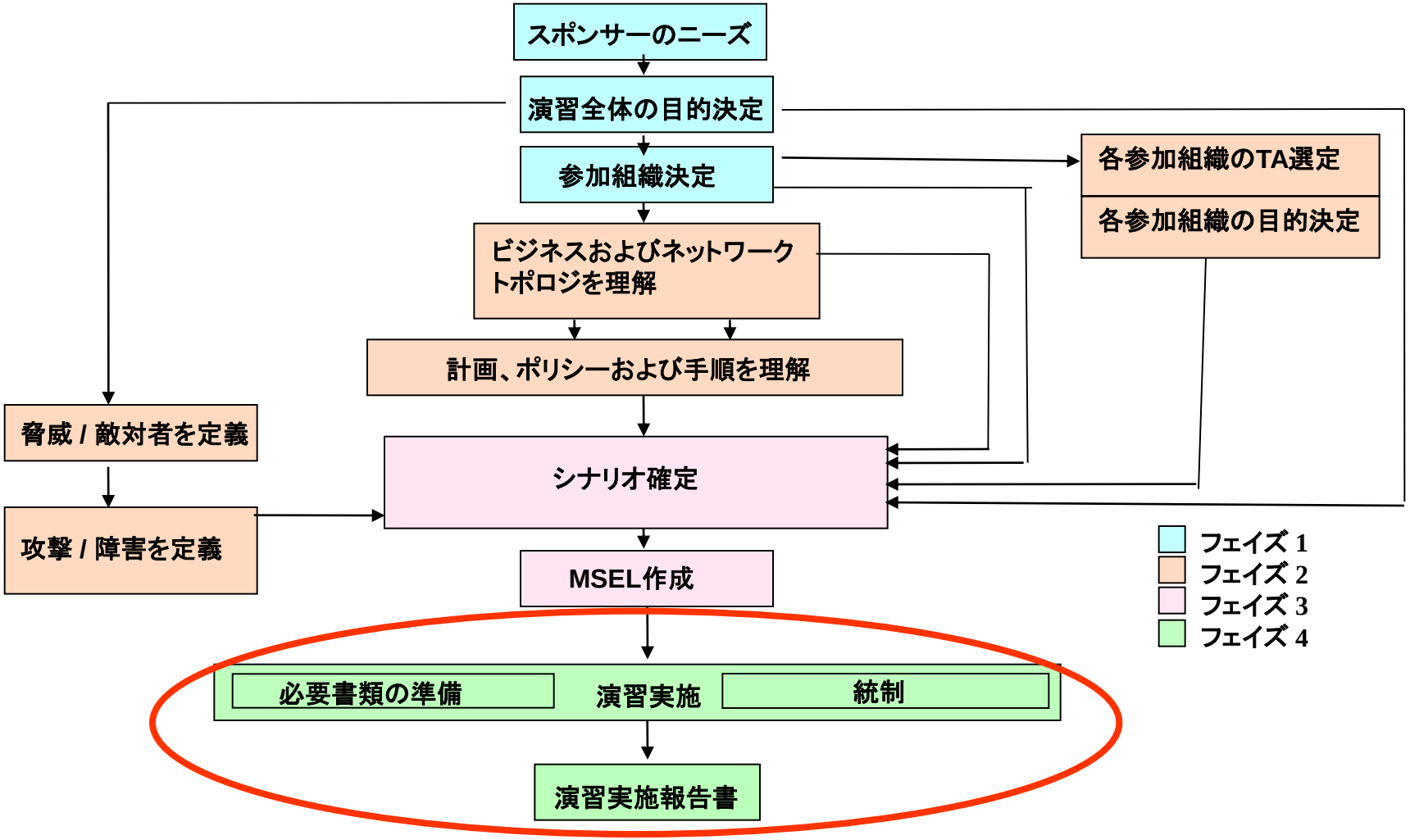
MSEL (Master Scenario Event List)の作成

・イベントのリストであるMSELを作成し、設定時間になったらツールで演習参加者に投入し、その内容に従い演習を実施します
・演習参加者はこのMSELほかに演習背景情報を持っていてそれも参照しつつ演習を進めます。

投入時間	イベント番号	イベント種類	投入タイミング	投入元	投入先	投入イベント	想定される行動	背景情報	備考
10:00	1M100	通常イベント	10:00になったら	ディレクター	参加者全員	演習開始します			
10:05	1M110	通常イベント	10:00になったら	ディレクター	重要インフラA社	指定する銀行に100万ドル振り込まないと、DDoS攻撃を開始する	警察、所管省庁に連絡	警察介入はなし	
10:20	1M120	通常イベント		ディレクター	重要インフラA社	予約受付Webに接続できない状態となる。	システムの調査を行う	DDoSが原因	
10:25	1M125	コンティンジェンシーイベント		ディレクター	重要インフラA社	CIOから連絡があった。接続ISPに対応依頼をするように			

一行ずつ順次投入

演習実施/報告書



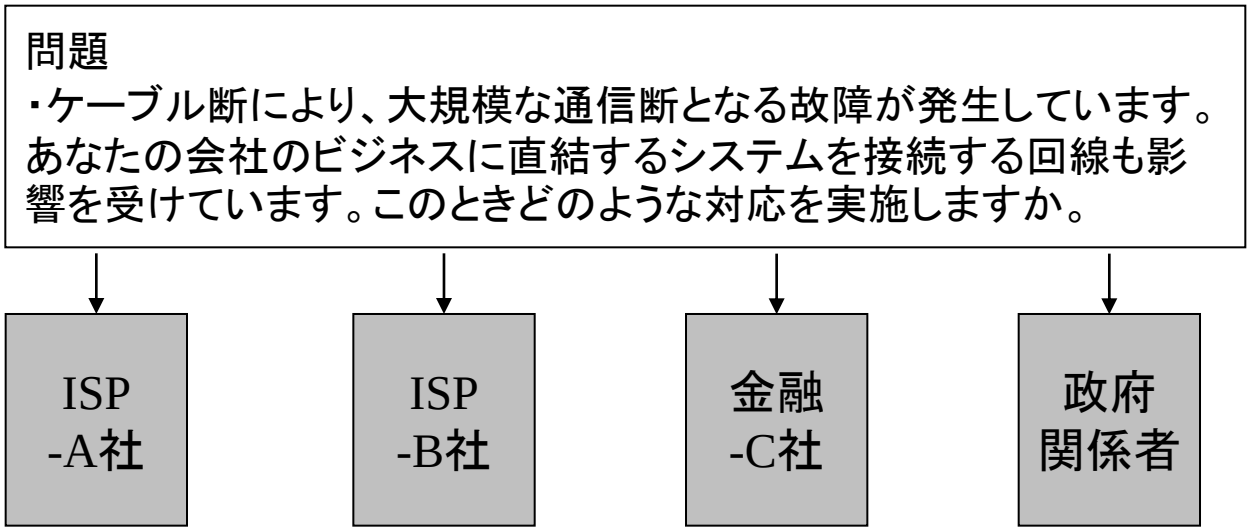
演習の実施直後に振り返りを行います
報告書を作成し、スポンサー、参加者等に提示します

簡単に演習を実施する方法はあるか

あります。

お題（問題）を出して、参加者に考えてもらい、話してもらうような問題集形式であると、演習設計の負荷はかなり少なくなります。

問題集形式の演習例：



各社で、いろいろなケースを想定して対応を話し合い、現状の運用の問題点を抽出する

この方式は、何年かでネタがすぐに尽きてしまう傾向にあります、また、各社の状況把握をしないので、実効性の面で弱い等の特徴があります。

簡単に演習を実施する方法はあるか

以前、サイバー攻撃対応演習にて実施した問題集形式の例（一部抜粋）

ある企業が海外の特定コンピュータが原因とみられるサイバー攻撃の被害者となった。このとき、この企業のとりうる選択肢は次のとおりである。

・社内と社外ネットワークの境界で攻撃を遮断しようと試みる

・その特定のIPアドレスからのトラヒックを遮断するよう、ISPに要求する

・攻撃をくい止めるために、攻撃元に対してハッキングし返す。

参加者への質問

1．攻撃の被害企業は、攻撃の対策としてISPからの支援を期待できるか

2．企業が受けた攻撃に対し反撃しようとする場合に発生しうる法制度上の問題は何か

3．日本国内の法律は、攻撃者が使用するテクノロジーに遅れをとることなく対応しているか

演習で勘違いしやすい点

－演習は、討議の結果やインシデント対応の良否を問うものではない。（演習の中心は議論）

～他企業より早い対応や解決を競うものでもありません

ライバル企業同士が集まると他社より早い対応を競ってしまうことがありますが。。

－プレイヤーの個人の評定を行うものではありません。

～当然スムーズにできなくてもよいのです。うまくいかないことを認識するのが演習の重要な部分です。

最後に：本日の話しのまとめ

第一段階：　演習に興味を持つ、必要であることを理解する

　演習を実施することにより、平時には体験できないインシデントを擬似体験、シミュレーションができる。また、次の内容が実施できることがわかった。

- 一次判断訓練～対応すべきインシデントであるか判断の訓練
- 二次判断訓練～自分で出来ること/対応すべきことの訓練
- 課題抽出～組織として、対応時に抜け落ちている事項の抽出

第二段階：　演習に参加してみたいと思う

　演習参加者はその効果を実感し、来年度も参加希望を持つことを理解した。何年か演習参加している企業であっても、対応環境や攻撃の変化により、業務運用のチェックが必要であり、定期的演習実施の必要性が確認されていることがわかった。

第三段階：　演習を企画、実施してみたいと思う

　演習を簡単に実施することも可能であるが、目的設定からMSEL作成までの手順を確実に踏み、また、TAを任命して参加各社の状況をよく調べてシナリオを設計することで、リアルで今後の改善につながる演習を実施できることがわかった。