NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

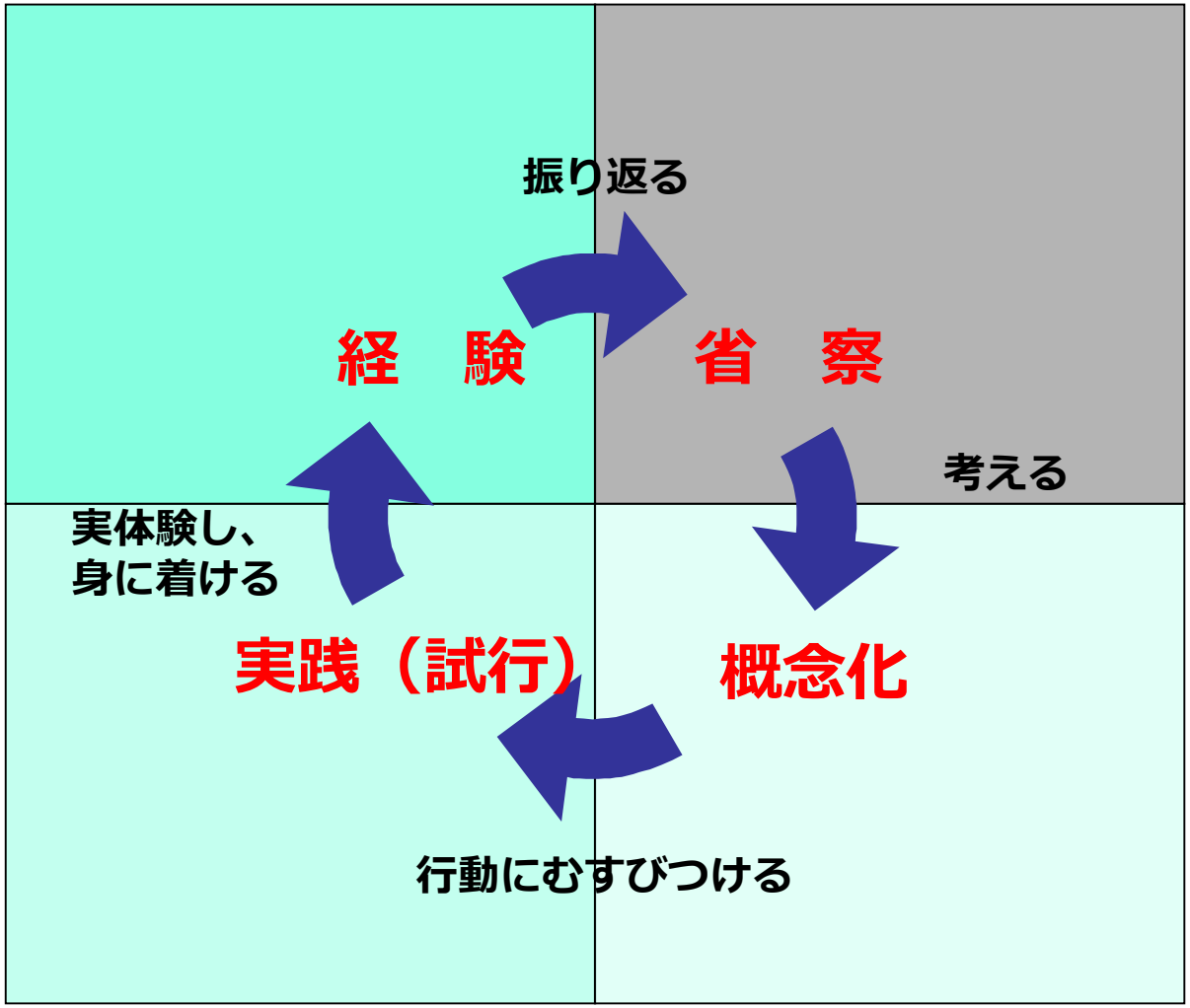
ゲーム演習による
実践的セキュリティ教育

2017年6月12日(月)

JNSA教育部会ゲーム教育WG
ラック　長谷川 長一
JPCERT/CC 輿石 隆

ゲームによる教育

ゲーム教育：経験学習



「経験学習モデル」～デビット・コルブ

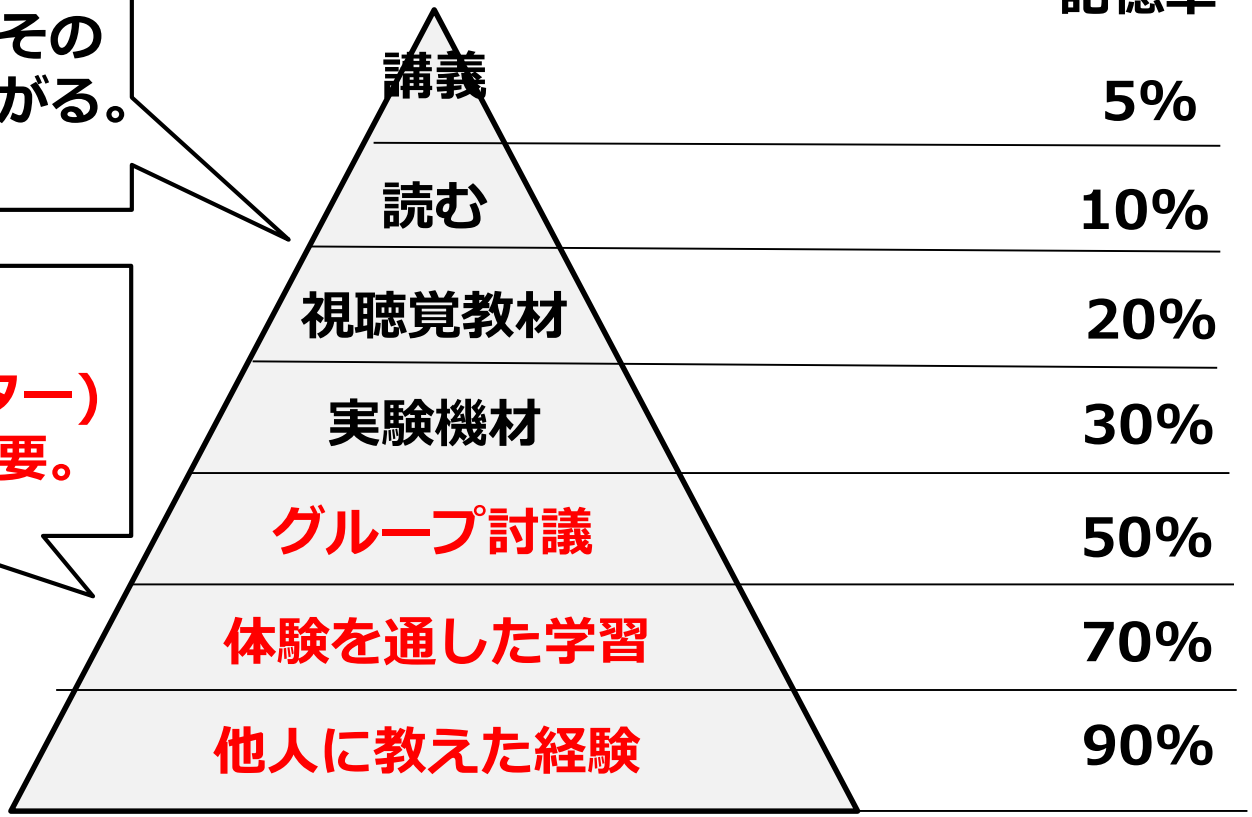
「経験学習」と「振り返り学習」

種　類	知識伝達学習	経験学習	振り返り学習
概要	正しい知識を持った人が、持っていない人に転移させて学ばせる	自らの体験や考察、他人の観察をもとに問題を解決しながら学ぶ	自らを振り返る（省察）することで、これから何をすべきかを学ぶ
メリット	・必要な知識を効率的に伝達できる。 ・多くの人を一度に学習させることができる。 ・未経験者や知識の少ない初心者にも教えることができる。	・自分の知識や経験が学習に生かしやすい。 ・受講者が主体的に学習できる。 ・具体的な「行動変容」に結びつけしやすい。	・受講者個々に合った「深い学習」が可能になる。 ・参加者同士の「学び合い」ができる。
デメリット	・内容が一律になりやすく、経験や知識のある者にとっては内容的に物足りなくなる。 ・講師主導のため、受講者の主体性が失われやすい。	・知識や経験の少ない人は学習しにくい。 ・一度に多くの知識やスキルを学ぶことができない。 ・過去の知識や経験から抜け出せないことがある。	・(講師など)外からの視点が入らないと、学びが広がりにくい。 ・学習の時間がかかり、効率が悪い。 ・受講者によって、差が出やすい。
学習形式	座学（スクール形式）	協働(ワークショップ形式)	協働(ディスカッション形式)

＜参考＞「ラーニング・ピラミッド」

教えることで、その人のスキルも上がる。

ここができる人(ファシリテーター)が、少ないが必要。



評価の指標

ゲーム教育の評価指標：RETAINモデル

要　素	概　要
R（Relevance） 実現性	ゲームがどれだけ現実に近いか
E（Embedding） 埋め込み	どれだけゲームの内容が学習 の内容と関連しているか
T（Transfer） 知識展開	得られた知識を他の文脈でも応用が可能かどうか
A（Adaptation） 知識取得促進	得られた知識から新しい知識を得ることを促すこと
I（Immersion） 積極的参加	参加者がどのくらい積極的にゲームに参加したか、相互的な関係がゲームの中に見られたか
N（Naturalization） 知識定着	得られた知識が定着し、その後も知識を利用すること

RETAIN model - Gunter et al. (2008)

JNSA開発のゲーム

JNSA開発ゲーム「セキュ狼」

「セキュ狼」とは？

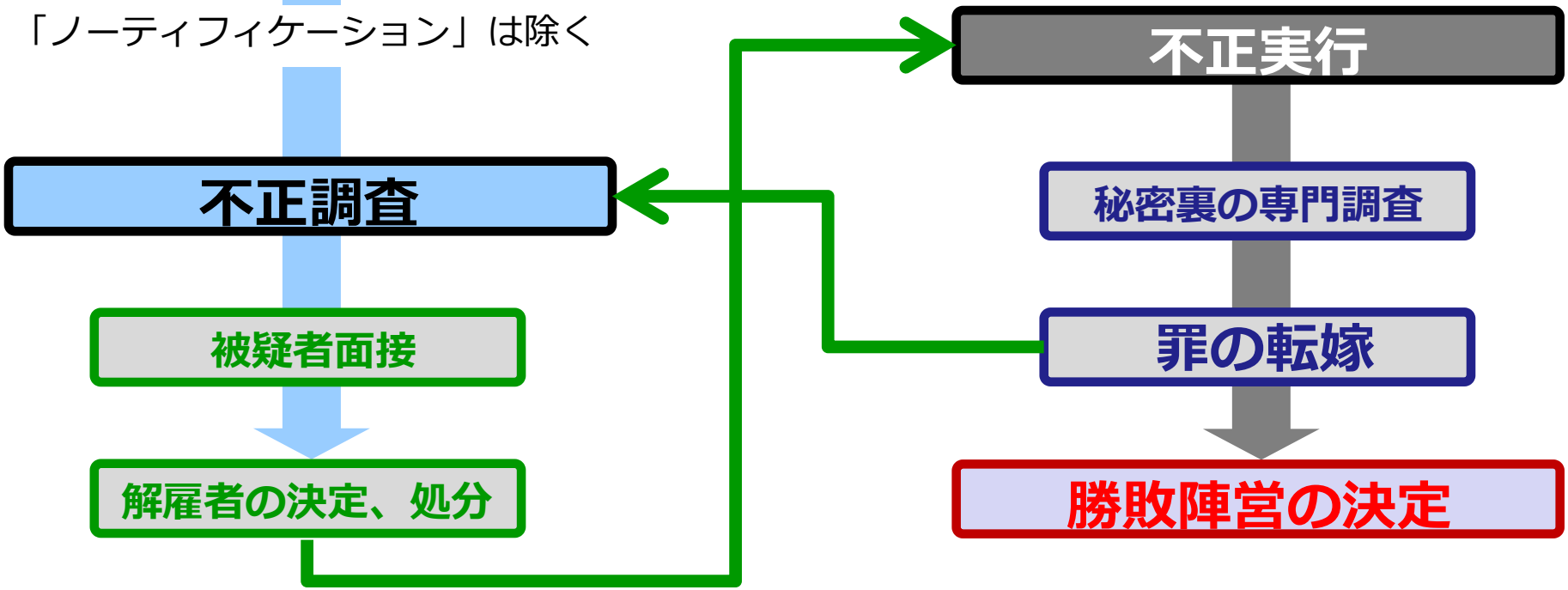
ハッシュタグ　#セキュ狼

ゲームの進行

同役職の相互確認

「ノーティフィケーション」は除く

勝敗陣営が決定するまで、
「不正調査」と**「不正実行」**を
ループし続ける。



教育ゲーム 第二弾！

ゲーム教育PJ オリジナル作品

「Malware Containment」

通称「MALCON」

プレイ人数：4～5人

プレイ時間：30分～60分

対象年齢　：13歳以上

難易度（前提知識の必要性）

難
- セキュリティベンダ制作物
- MALCON
- セキュリティ専門家人狼

易

ゲームテーマと学習内容

テーマ

外部からの通報を受け、PC 端末を調査し、マルウェアに感染した端末を特定、「封じ込める」までの初動対応をイメージした。

学習内容

CSIRT の役割と、所属する人材、人材が持つ機能について学ぶ。

コマンダー

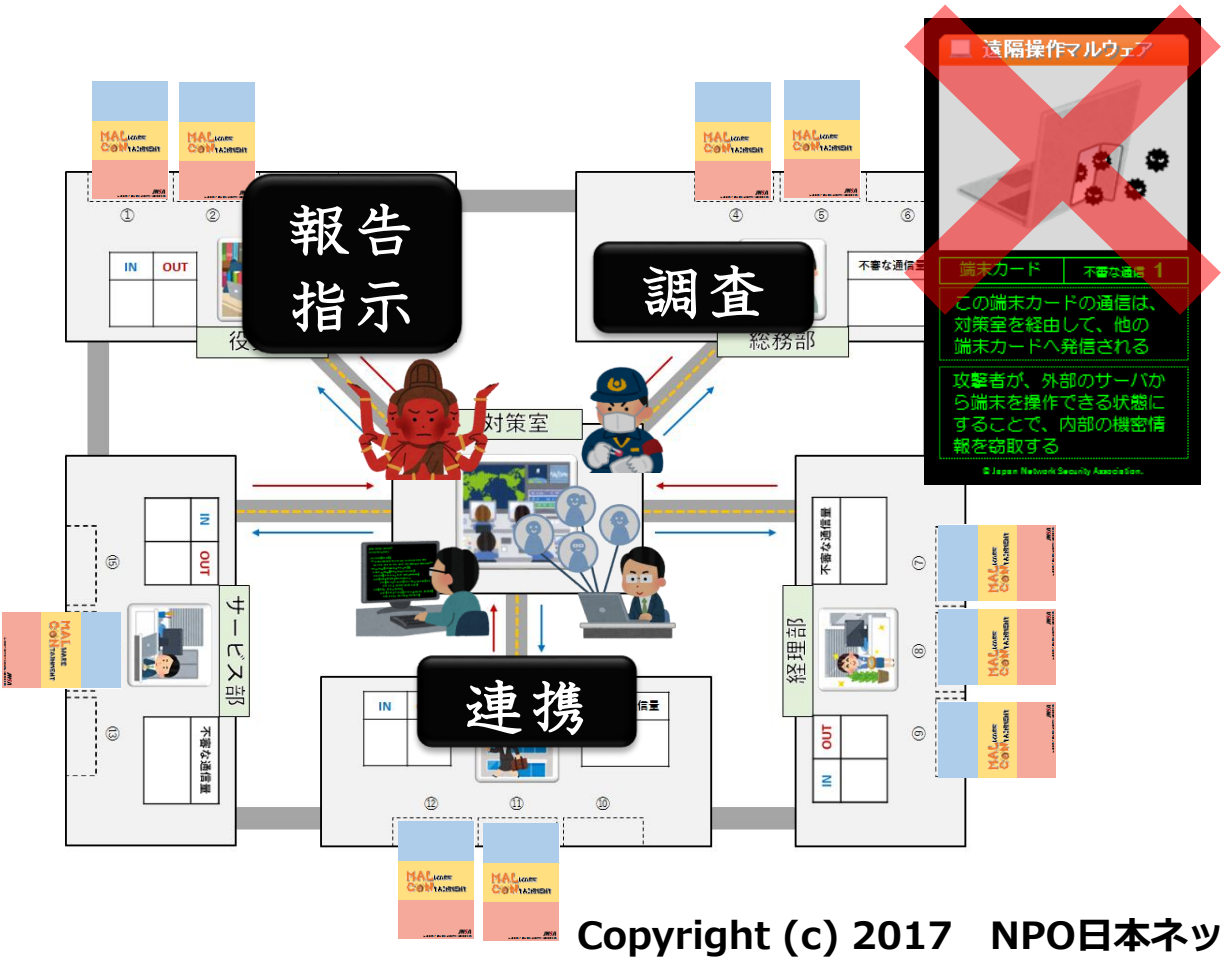
フォレンジック
エンジニア

リサーチャー

ノーティフィ
ケーション

ゲーム概要

プレイヤーは、各部署への移動や役職固有の能力を駆使し、10枚の端末カードの中から2枚の遠隔操作カードを発見し、封じ込めることができれば勝利となります



ゲーム中は会話が制限され基本的に同じ部署にいるメンバー間でしか、情報交換できない仕組みです

自らの持つ能力を理解し迅速に情報連携する事が勝利の鍵となります

効果について考える

学生・新人教育向け

- セキュリティに係る被害や CSIRT という組織が持つ役割の学習
- チームや報告体制の重要性に関する学習
- 会話や情報交換ができない中で、何が最適な行動か「考える」こと

経営層・CSIRT 向け

- 自分達の組織だとどうなのか振り返る
  - 人的な部分
  - 対応フローの部分
  - 速度的な部分
- 経営層の考えを(自然に)聞き出せる
- 自身の活動に関する理解を深められる

近日、公開！

■ もうしばらくお待ちください！

実証実験や演習・体験会の実施

ゲーム教育を効果的にするには

振り返り学習のフロー例

パターン・その1

(1) • 講義（Lecture）

(2) • 協働（Workshop）

(3) • 省察（Reflection）

パターン・その2

(1) • 協働（Workshop）

(2) • 省察（Reflection）

(3) • 講義（Lecture）

振り返り学習(パターン1)

学習目標の設定（知識、技術、コンピテンシー等）

事前学習

ゲーム学習の実施(1回目)

振り返り、目標に対する成果の評価、目標の更新(1回目)

ゲーム学習の実施(2回目)

振り返り、目標に対する成果の評価、目標の更新(2回目)

振り返り学習(パターン2)

学習目標の設定（知識、技術、コンピテンシー等）

ゲーム学習の実施(1回目)

振り返り、目標に対する成果の評価、目標の更新(1回目)

事後学習

ゲーム学習の実施(2回目)

振り返り、目標に対する成果の評価、目標の更新(2回目)

キューブリック評価の例：知識

大項目	中項目	小項目
セキュリティ対策技術	□ファイアウォール □侵入検知 □認証 □・・・	□・・・ □・・・ □・・・ □・・・
セキュリティサービス	□監視 □診断 □運用 □・・・	□・・・ □・・・ □・・・ □・・・
脅威	□標的型攻撃 □DDoS攻撃 □フィッシング □・・・	□・・・ □・・・ □・・・ □・・・

キューブリック評価の例：コンピテンシー

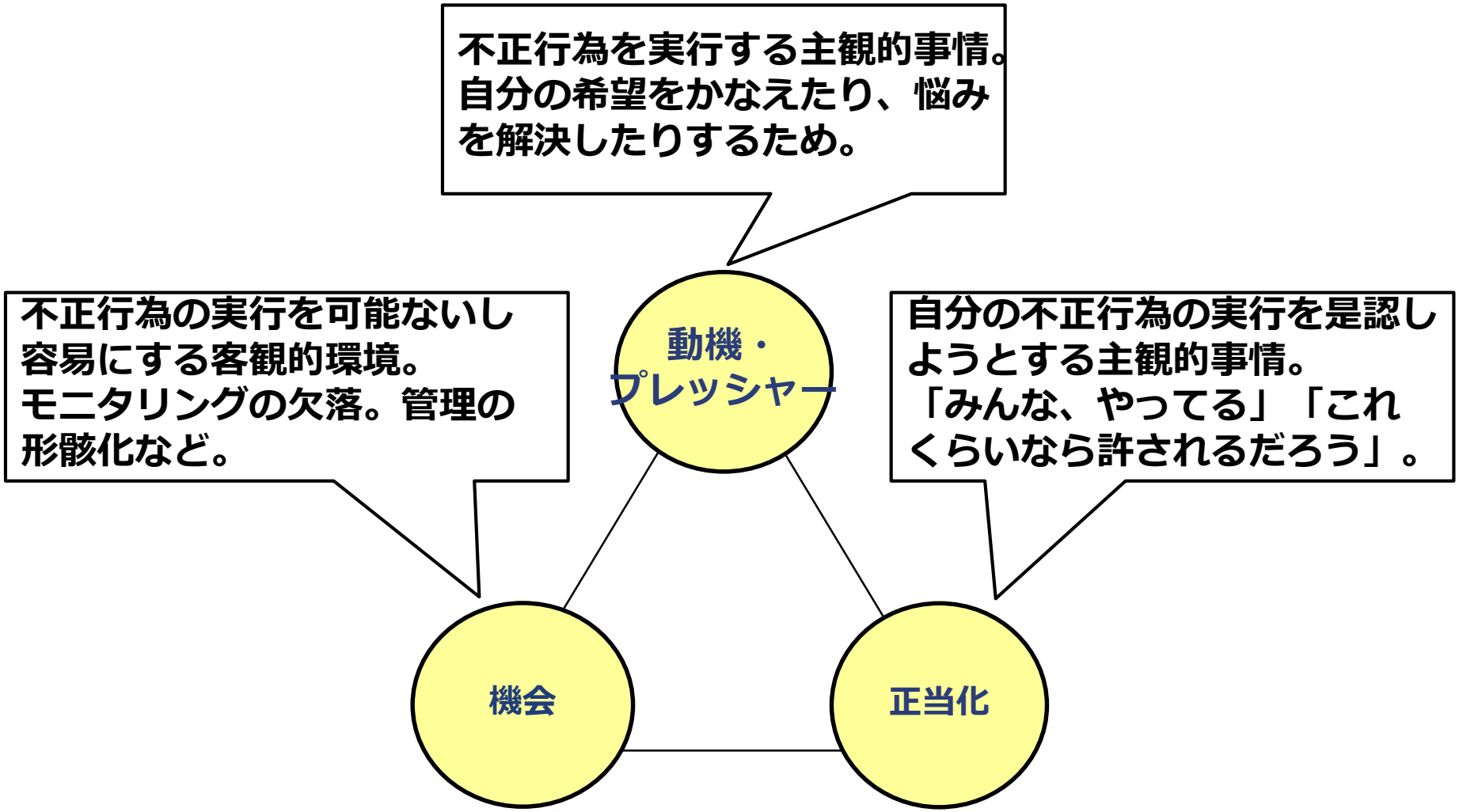
コンピテンシー	評価基準	重み
状況判断力	□チームが置かれている状況を適切に把握し、判断に結びつけることができたか □・・・	15%
コミュニケーションカ	□チームメンバーと円滑なコミュニケーションができたか □・・・	10%
意思決定力	□チームの戦略や方針に基づき、意思決定を行うことが出来たか □・・・	10%

キューブリック評価の例：アクティビティ

	質的評価項目	量的評価項目
行動	重み：25% (1) 発生したイベントについて、適切かつ迅速に判断できたか。 (2)・・・	重み：25% (1) 発生したイベントの影響度について、半数以上を影響度20%以下に低減できた。 (2)・・・
成果	重み：25% (1)・・・ (2)・・・	重み：25% (1)・・・ (2)・・・

振り返り学習の例
-「セキュ狼」の場合-

「不正のトライアングル」



ソーシャルエンジニアリング

JNSA

　攻撃や不正行為をするために必要となる重要な情報を、IT技術を使用せずに盗み出す方法。

　その多くは人間の心理的な隙や行動のミスにつけ込みだますもの。

不正行為者のプロファイリング

　不正行為者には、ある程度の共通した行動特性がある。

　不正行為が行われた場合は、何らかの「前兆」や「痕跡」がある。

状況的犯罪予防論(SCP)

「状況的犯罪予防論(Situational Crime Prevention:SCP)」5つの観点

	観　点	具体的な対策の例
1	物理的にやりにくい状況を作る	犯罪の対象物を強化すること。家庭の泥棒対策では、防犯ガラスや不正解錠に強いカギを導入することなど。
2	やると見つかる状況を作る	死角をなくす、人々の防犯意識を高めることで、侵入する行為が見つかる機会を増やすなど。
3	やっても割に合わない状況を作る	泥棒によって得られる利益を少なくすること。盗まれるものを家に置かない、名前を書くことで盗品を転売できなくするなど。
4	その気にさせない状況を作る	泥棒する気を起こさせない対策。現金や宝飾品などが外部から見えないようにするなど。
5	言い訳を許さない状況を作る	犯罪者に都合の良い「言い訳」を許さないようにすること。

まとめ：これからの実践的教育

- まず、実践的教育ができる人材の育成と維持が必要。（教える人は現役かつ現場の業務を知っている者）
- 育成した人材の活用のための環境や体制の構築と維持も必要。
- チャレンジできる場(機会)、失敗できる場をできるだけ多く提供すること。
- 欠点を見つけ修正する教育ではなく、長所を見つけ伸ばしていく教育。

組織的、かつ継続的な教育と支援が必要

まずは、ゲーム教育を始めてみてください！
http://www.jnsa.org/edu/secgame/