

コミュニケーションで乗り切れ！ サイバーインシデント対応24時

CYBER SECURITY COMMUNICATION

ゲーム説明書

プレイ人数	4人～6人
プレイ時間	1時間程度
対象者	サイバーインシデント対応関係者

1. ゲームの目的

本ゲームはサイバー攻撃発生時のインシデント関係者として適切な対応・情報共有を行うことを目指します。

【教育効果】

- ・インシデント発生時の組織連携の重要性を学ぶ
- ・適切に情報共有を行うことの重要性を学ぶ
- ・組織間連携に必要な事前調整事項について学ぶ

2. コンポーネント



役割カード(全5種)

【説明】それぞれの役割情報が記載されています。

- 【情報】①:役割名称
②:担当業務・役割
③:役割の特性・立場
④:抱える問題点



行動カード(全41種)

【説明】サイバー攻撃に対して行う行動です。行動カードを同じ番号の情報カードを入手できます。

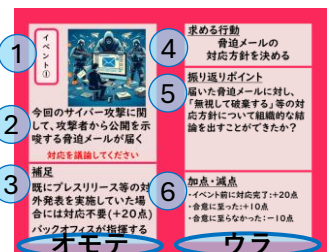
- 【情報】①:カード番号・概要
②:行動実行者
③:具体的な内容
④:補足



情報カード(全41種)

【説明】行動に応じて得られる情報です。次の行動に繋がる手がかりが記載されています。

- 【情報】①:カード番号・概要
②:具体的な内容
③:補足



イベントカード(全11種)

【説明】一定確率で発生し、メンバーで対応を議論します。

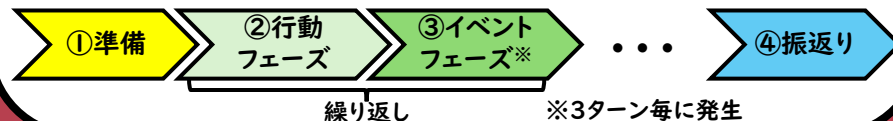
- 【情報】①:カード番号
②:イベント内容
③:イベントの補足内容
④:求められる行動
⑤:振り返り時のポイント
⑥:得点

3. ストーリー

あなたたちはとある製造業の会社で働いています。近年、サイバー攻撃を受ける会社が多く、自社でも対策を推進しています。しかしある日、社内でサイバー被害が発生しました。関係者で情報連携を行い、インシデントを上手く乗り切りましょう。

4. ゲームの流れ

- ・ゲームは大きく4つのフェーズで構成されています。
- ・行動フェーズで参加者毎に実行することは以下の2つです。
 - ー「行動カード」の使用による「情報カード」入手
 - ー「情報カード」の他参加者への共有
- ・イベントフェーズで参加者が実行することは以下です。
 - ー「イベントカード」への対応を全員で議論
- ・行動フェーズとイベントフェーズを繰り返し、事態の收拾を行います。



5. ゲームの進め方

①準備

- ・役割を決めて、「役割カード」と「行動カード」を配布します。
 - ープレイヤー6人:CSIRTを2人とし、5つの役割を決める。
 - ープレイヤー5人:一人一役とする。
 - ープレイヤー4人:IT部門とバックオフィスを一人が兼任する。
- ・「情報カード」をテーブル上に裏返して山札として置きます。
- ・「イベントカード」はシャッフルして表向きで山札として置きます。
- ・上記が完了し、情報カード⑩を現場担当が引くところからスタートします。

②行動フェーズ

- ・工場(工場長/現場担当)が最初にアクションをします。
(工場長/現場担当はお互いに何度もアクション可能)
- ・工場→IT部門→バックオフィス→CSIRTの順番です。
- ・CSIRTまで終了すると行動フェーズが終了になります。
- ・具体的なアクションは以下の通りです。
 - ー自分が保有/テーブル上(全体共有された)の「情報カード」を基に「行動カード」を使用します(使用に条件が記載されている場合もある)。
 - ー「行動カード」を使用すると、同じ番号の「情報カード」を入手します。
 - ー入手した「情報カード」をその情報が必要な人に渡します。
(「行動カード⑩」により、1度だけ複数の情報カードを全員に共有可能。)
 - ー一度相手間違えた場合、次の順番で改めて渡し直すことができます。
 - ー上記を繰り返し、アクションすることがなくなれば自分の番は終了です。



③イベントフェーズ

- ・行動フェーズが3周する毎にコインを投げ、表が出ると以下を実施します。
 - ー「イベントカード」を無作為に1枚引き、対応を2分間議論します。
- ・コインが裏面か、2分経過、議論が終了すると本フェーズは終了になります。
- ・初回や難易度が高いと感じた場合、実施しなくても影響はありません。

終了(振り返りは裏面に記載)

- ・行動フェーズとイベントフェーズを繰り返し、インシデントの封じ込め・復旧見込みが立ち体制解除の時点でゲーム終了です(情報カード④⑩に記載)。

コミュニケーションで乗り切れ！ サイバーインシデント対応24時

CYBER SECURITY COMMUNICATION

5. ゲームの進め方(続き)

④振り返り

1. 制限時間(40分以内)でどこまで実施できたかで点数を決めます。

- ーサイバー攻撃と判断(情報カード⑬) 25点
- ー封じ込め計画の立案(情報カード⑳) 50点
- ー会計システム復旧(情報カード㉑) 75点
- ー特別体制の解除(情報カード㉒) 100点

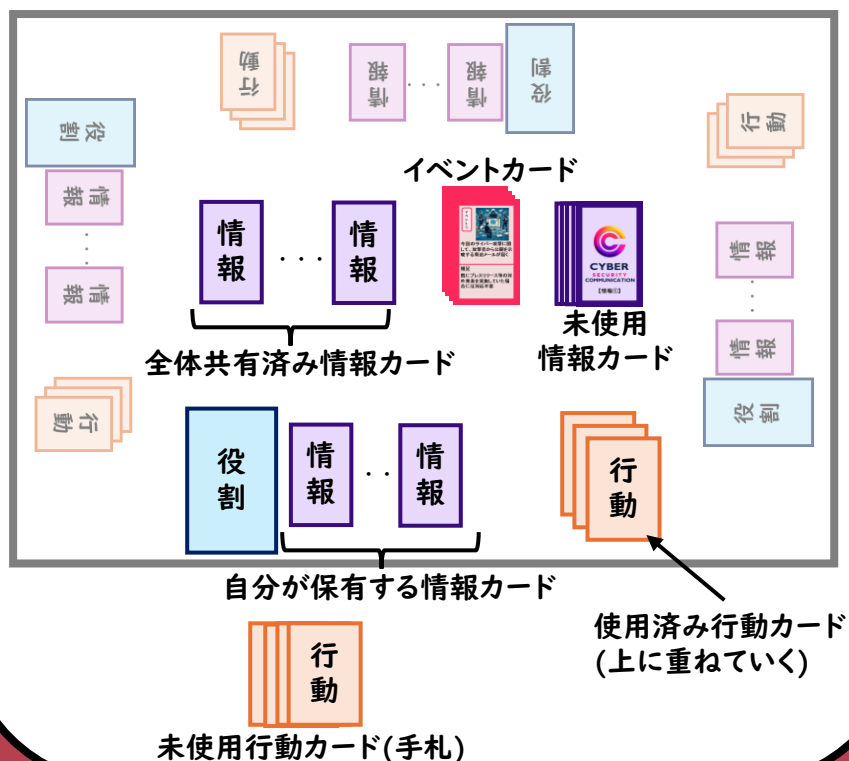
2. 次に使用したイベントカードの裏面を確認し、各イベントごとの加減点を計算します。

3. 参加者でコミュニケーションの良かった所を共有します。
(ex.あのタイミングで情報が来たからスムーズにできた。)

4. コミュニケーションの改善点を共有します。
(ex.行動しなかったけど、情報がこなくて出来なかった・・・。)

5. 自社でインシデントが発生した際の動きと比べて、自社の方が良くできているところ、改善が必要なところを右のチェック表を参考にしながら議論してください。
(ex.自社ではこの意思決定は経営層ではなく工場長でできる。)
(ex.広報のプレス準備等、具体的な連携ができていない。)

参考. カードの置き方(例)



参考. 振り返りチェック表

チェック項目	☑
NIST "Computer Security Incident Handling Guide"	
コミュニケーションツールの優先順位が確立され、関係者に周知されている	
緊急時の連絡先情報が用意されており、常に最新情報に更新されている	
インシデント対応の情報を一元管理するフォーマットが存在している	
連携が必要な外部機関およびその連絡先が整理されている	
インシデントの重要度を決める指標があり、関係者に周知されている	
SANS Institute "Incident Handler's Handbook"	
演習を通じてインシデント対応組織の課題を発見し改善する仕組みがある	
インシデント対応を記録するフォーマットがあり分析できる仕組みがある	
誰がどのようにインシデントを報告するか、どの情報を含めるべきか定められている	
インシデント終了後に振り返りを実施している	

上記はサイバーセキュリティに関するガイドライン等から、インシデント対応時のコミュニケーションや組織間連携について記載されている部分を一部抜粋/要約して掲載しております。詳細は元ガイドラインをご確認ください。

参照元：

NIST "Computer Security Incident Handling Guide"

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

SANS Institute "Incident Handler's Handbook"

<https://www.sans.org/white-papers/33901/>

本コンテンツで利用しているイラスト・画像は全て生成AI(ChatGPT4.0)にて作成しております。

制作：ICSCoE 7期生 セキュリティ啓発コンテンツPJ