



# セキュリティホライゾン

## ～ここから始めるIoTセキュリティ～

### 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	システム開発・導入組織

## 1. ゲームの目的

本ゲームはDXの推進により急激に広がったクラウドやIoT等のシステムに対して起こりうる被害とその対策を理解することを目指します。

### 【教育効果】

- サイバー攻撃による被害とその原因の関係を理解する
- サイバー攻撃被害を防ぐためのセキュリティ対策を理解する

## 2. ゲームの流れ

- ゲームは大きく3つのステップで構成されています。
- 「原因検討」で参加者が実行することは以下です。
  - 被害カードの記載内容から、その被害が発生した原因を推察する。
  - 推察を繰り返し、カードに記載されている原因にたどり着く。
- 「対策検討」で参加者が実行することは以下です。
  - 被害カードに記載されている原因への対策について、手持ちの対策カードを参考にして検討する。



## 3. ゲームの進め方

### ①準備

- ゲームマスター (GM) 1名を選出する。
- 業務の特性などから被害カード 表面(全6種)から1種類を選択する。

### ②原因検討

- メンバー: 原因を特定すべく、GMにYESorNOで回答可能な質問をする
- GM: メンバーの質問に対し、YESorNOor不明で回答する
- メンバーが原因を当てることができた場合、次のステップに移行する。

### ③対策検討

- メンバーは被害や原因をもとに有効と思われる対策カードを選出する。
- 選出完了後、被害カードの裏に記載されている対策一覧をもとに答え合わせを実施する。

## 4. コンポーネント

**被害**



1 前提:  
個別システムとなっていた経理システムを、クラウド上に経理統合基盤として統合した。

2 被害:  
公開前の決算情報が漏洩していることが判明した

3 #経理部門 #決算情報 #情報漏洩

### 被害カード 表面(全6種)

#### 【説明】

被害内容について記載されています。

#### 【情報】

- ①: システムの前提となる背景・説明
- ②: システムで発生した被害について
- ③: カードと関連するキーワード

1 原因: アカウント管理不足により、不正アクセスされた

2 対策:  
・不要なアカウントの削除を実施  
・クラウドの公開設定を社内のIPに限定  
・アカウントの適切な権限設定

3 今回の経緯:  
企業に恨みをもったまま経理部社員が退職  
退職した経理部社員のアカウントが削除されずそのまま放置されていた  
退職した経理部社員が、退職後クラウド上の経理システムにアクセスしたところ、インターネット上からアクセス可能であった  
経理システムにアクセスし、公開前の決算情報のデータをダウンロード  
退職者が競合企業に公開前の決算情報のデータを売買した

### 被害カード 裏面(全32種)

#### 【説明】

被害発生の原因と対策、被害までの経緯が記載されています。

#### 【情報】

- ①: 今回の被害を引き起こした原因
- ②: 被害原因への対策内容
- ③: 被害が発生するに至った経緯

**対策**



1 初期認証情報(パスワード等)の変更

### 対策カード 表面(全24種)

#### 【説明】

セキュリティ対策の簡単な説明が記載されています。

#### 【情報】

- ①: セキュリティ対策の概要

1 初回ログイン時に最初に設定されている認証情報(パスワード等)を強制的に変更させる。

2 初期パスワードは製造時に設定されているもので、共通のパスワードが用いられていることが多くあります。  
これを放置すると外部からの攻撃者による不正アクセスのリスクが高くなります。  
このリスクを防ぐために、システム上で初回ログイン時に強制的に変更させる機能を実装することも重要な対策になります。

### 対策カード 裏面(全24種)

#### 【説明】

セキュリティ対策の説明や対策が必要な理由、考え方が記載されています。

#### 【情報】

- ①: セキュリティ対策の具体的な内容が記載
- ②: 当該セキュリティ対策の詳細が記載

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。