IoT・ポリー

IoT セキュリティ演習用カードゲーム

ゲームマニュアル Ver.1

奈良先端科学技術大学院大学
サイバーレジリエンス構成学研究室

目次

1 はじめに

1. 1 IoT・ポリーについて

カードゲーム形式で IoT の脅威分析について学習するための演習用ツールです. IoT カードとアタックサーフェスカードを組み合わせることで様々な IoT 環境を想定できます. 脅威と対策カードを用いて想定した環境の脅威と対策について学習します.

1. 2 ゲームの目的・目標

ゲームの目的:カードゲーム形式で IoT の脅威分析方法について学びます. また, カードに記載された具体的な脅威と対策について, 知識を得ることができます.

ゲームの目標:想定された IoT 環境において最も深刻な脅威をプレイヤー間の議論を通じて考察します. また, 想定される脅威への有効な対策と残留リスクを議論により考察します. グループによる作業を実施することで協調的な行動が必要になります.

1. 3 ゲームの対象

情報セキュリティに関心があるすべての方が対象です.

当然, 情報セキュリティに知見を有している人のほうが容易にゲームを進捗できますが, 情報セキュリティの知見を有していなくても, 他の方との議論により多くの知識を共有できます.

1. 4 参加人数・時間

プレイヤー:3～7 人(基準)

ゲームマスター:1 名(情報セキュリティの知見を有する人が望ましい. ゲームの進捗や参加者がカードの記載内容がわからなかった場合に助言を行います.)

時間:1 時間(基準. 連続して演習を実施する場合は, 適宜休憩をいれてください.)

2 カード

本ゲームで使用するカードは IoT カード, アタックサーフェスカード, 脅威カード, 対策カードの 4 種類です. それぞれのカードの詳細は下記のとおりです.

2. 1 IoT カード

IoT カードは用途に応じて, 10 種類のカードにまとめています. 図1にカードのイメージを示します. カードの上部にはタイトルを記載しています. カードの中央部にはタイトルで示した IoT の概要を記載しています. カードの下部には 5 つの特徴(機密性, 完

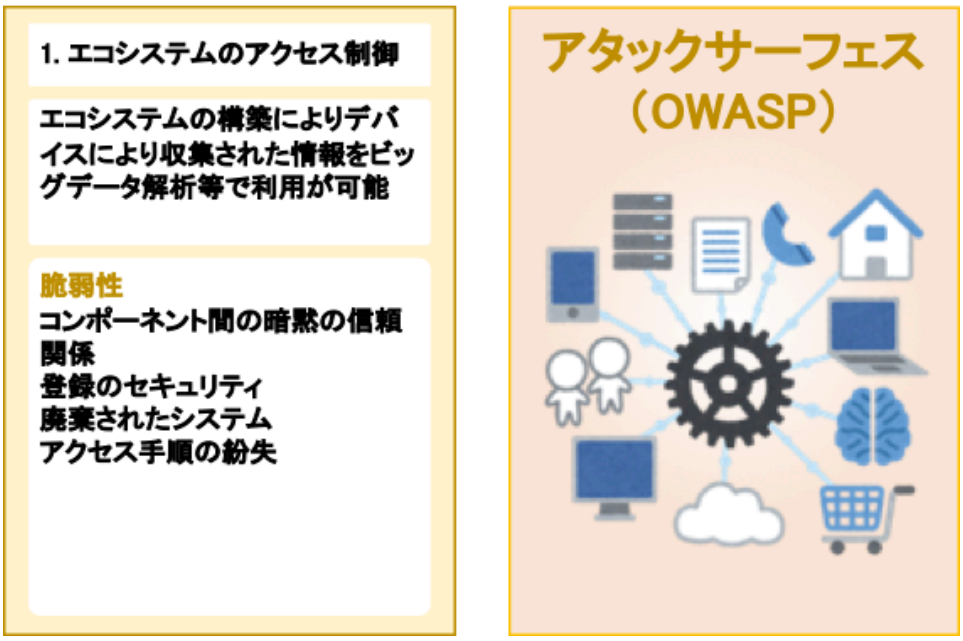
全性，可用性，セーフティ，プライバシー）が空欄になっています．参加者の議論によりシステムの概要とシステム構成図から優先度に順位付けします．

表面　　裏面

図 1　IoT カード

2. 2　アタックサーフェスカード

アタックサーフェスとは，サイバー攻撃の対象となり得る領域のことを言います．本ツールでは OWASP Internet of Things Project で定義された IoT の代表的な 18 個のアタックサーフェスをカード化しています．図 2 にアタックサーフェスカードのイメージを示します．カードの上部にはタイトル（アタックサーフェス名）を記載しています．カードの中央部にはアタックサーフェスの概要説明を記載しています．カードの下部にはアタックサーフェスの代表的な脆弱性を記載しています．



表面　　裏面

図 2　アタックサーフェスカード

2. 3　脅威カード

脅威カードはサイバー攻撃手法の辞書にあたる CAPEC™ のメタ抽象化に該当する内容を 61 枚のカードにまとめています．図 3 に脅威カードのイメージを示します．カードの上部には脅威の内容を記載しています．カードの中央部には脅威の概要説明を記載しています．カードの下部には脅威の詳細な攻撃手法名を記載しています．

表 1 に脅威カード補足資料（一部抜粋）の内容を示します．CAPEC™ ではサイバー攻撃手法の抽象度に応じて 3 つに分類（メタ抽象化，標準抽象化，細部抽象化）しています．脅威カードの記載内容にあたるメタ抽象化は最も抽象的な内容となっており，プレイヤーによってカード内容から具体的な攻撃手法をイメージすることが困難な場合があります．このため，脅威カード補足資料には CAPEC™ の標準抽象化の内容を一覧にしてまとめています．プレイヤーは脅威カードの具体的な攻撃手法を確認する場合，攻撃カードの CAPEC ID 番号から脅威カード補足資料で記載された具体的な攻撃手法を確認することができます．

表面　　裏面

図 3　脅威カード

表 1　脅威カード補足資料

CAPEC ID	タイトル	関連項目	概要
21（脅威カード）	信頼できる資格情報の悪用	アクセス制御を破棄する	セッション ID とリソース ID への攻撃は、一部のソフトウェアが信頼性を確認せずにユーザの入力を受け入れるという事実を利用しています。・・・
21 196	セッションクレデンシャルの改ざん	信頼できる資格情報の悪用	攻撃者は、サービスへのアクセスを取得または侵害するために、偽の機能的なセッションクレデンシャルを作成します。・・・
21 593	セッションハイジャック	信頼できる資格情報の悪用	この攻撃には、認証の実行時におけるアプリケーションのセッション使用の弱点を悪用する攻撃も含まれます。・・・

2. 4　対策カード

対策カードは ENISA（欧州ネットワーク・情報セキュリティ機関）により作成された IoT セキュリティ対策のグッドプラクティスである Baseline Security Recommendations for

IoT のリスク低減策を 71 枚のカードにまとめています. Baseline Security Recommendations for IoT では様々な IoT の共通的な対策がまとめられており, IoT の特徴に応じて必要なグッドプラクティス内のセキュリティ対策を講じることでリスク低減を図ることができます. 図 4 に対策カードのイメージを示します. カードの上部に対策名を記載しています. カードの中央部には対策の概要を記載しています. カードの下部には主な脅威対象を記載しています.

表面　　裏面

図 4　対策カード

3　ゲームのルール

3. 1　ゲームサイクル

ゲームサイクルは以下のとおりです.

(1)プレイヤーに脅威カードと対策カードを 10 枚ずつ配布します.

(2)任意のプレイヤーが IoT カードを引き, 提示します. (または, プレイヤー間で IoT カードを選択します.)

(3)プレイヤー間の議論により, 機密性, 完全性, 可用性, セーフティー, プライバシーの優先度を定義します.

(4)任意のプレイヤーがアタックサーフェスカードセットから 1 枚のカードを引き, 提示します.

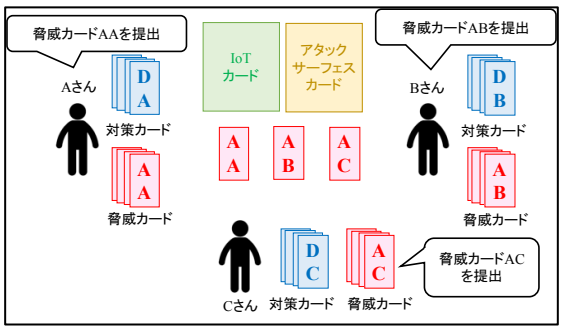
※別に配布したシステム構成図の対象箇所を使って，以降の検討を行うとイメージしやすくなると思います．
(5)プレイヤーは，提示された IoT カードとアタックサーフェスカードから想定される最も深刻な脅威を手持ちの脅威カードから 1 枚選択し，提出します．手持ちの脅威カードから選択できない場合，脅威カードセットから最大で 5 枚のカードを追加で引くことができます．
(6)最も深刻な脅威に選ばれた脅威カードを使ってリスクシナリオをワークシートに記載します．
(7)プレイヤーは記載された 1 つのリスクシナリオから，最も効果的であると考えられる対策を手持ちの対策カードから提出します．手持ちの対策カードから選択できない場合，対策カードセットから最大で 5 枚のカードを追加で引くことができます．
(8)プレイヤー間の議論により，提出されたカードを対策の効果順に順位付けします．
(9)ワークシートに提出された対策カードと順位付けの理由を記載します．
(10)プレイヤーは提出したカードから残留リスクを議論します．残留リスクの許容可否と残留リスクを許容できない場合の追加の対策についてワークシートに記載します．
(11)(3)～(10)をアタックサーフェスの回数繰り返します．
(12)(11)でゲームは終了ですが別の IoT カードを使って，(1)～(11)を再度繰り返すことでゲームを継続することも可能です．

3．2 ワークシートについて

ゲームサイクルの進行に従い，ワークシートに提出した脅威カードや対策カード，リスクシナリオ・残留リスクの記録を行います．ゲーム終了後，ワークシートを確認することで振り返りが可能です．

3．3 ゲームイメージ

プレイヤーがルールを理解できるようにするため，ゲーム進行のイメージを 4 コマにまとめて，図 5 に示します．

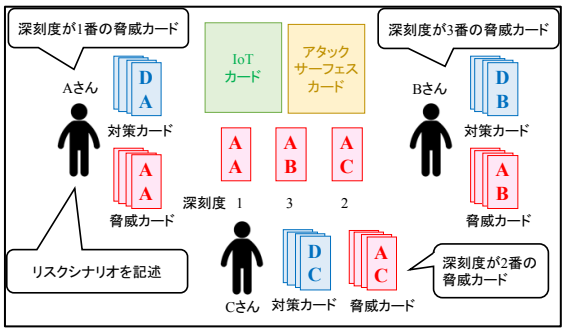


1コマ目

・プレイヤーに脅威と対策カードを配布

・IoT・アタックサーフェスカードを提示

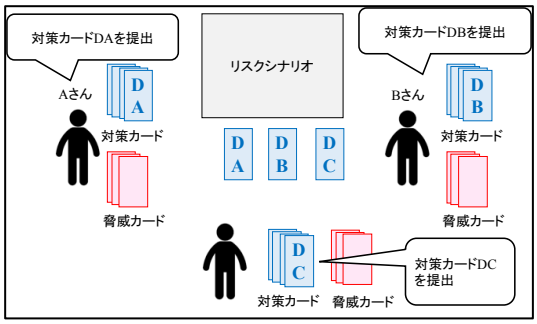
・最も深刻な脅威カードを提出



2コマ目

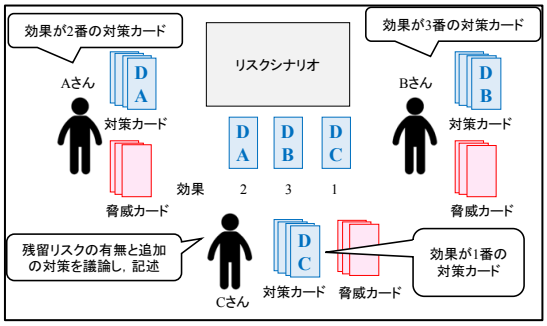
・脅威カードに深刻度の順位付け

・リスクシナリオを記述



3コマ目

・最も効果的な対策カードを提出



4コマ目

・対策カードに効果の順位付け

・残留リスクの分析

図5　ゲーム進行のイメージ（4コマ）