IoT-Poly

Game Manual Ver.1

Nara Institute of Science and Technology
Laboratory for Cyber Resilience

1. What is “IoT-Poly”?

This is an exercise tool to learn about threats and countermeasures of IoT by experiencing IoT risk assessment process.

1.1 Overview of Cards

There are four types of card sets, IoT cards, attack surface cards, threat cards and countermeasure cards. The attack surface cards contain 18 attack surfaces summarized by the OWASP IoT Project. Threat cards contain a list of Meta Abstractions on CAPEC which is one of the attack library. Countermeasure cards contain the contents of Baseline Security Recommendations for IoT summarized by ENISA.

Rule (1/2)

1.2 Rule

(1) 10 threat cards and 10 countermeasure cards are distributed to the players.

(2) A player draws and presents an IoT card. (Or players select it.)

* * * This time we will distribute it in advance. * * *

(3) A player draws and presents one card from the attack surface card set.

* * * It becomes easier to image with the relevant part of the use case diagram when conducting subsequent process of the game. * * *

(4) Players select and submit one threat card that matches the most serious threat envisioned from the IoT card and attack surface card. Player can draw up to five additional cards from the threat card set if they cannot submit their card. A player does not have to submit a threat card if there are still no cards to submit.

(5) Players rank the cards submitted in order of seriousness of the threats through discussions among them.

(6) Players consider and write a risk scenario that is assumed from the most serious threat card on the worksheet.

(7) Players submit a countermeasure card that is considered the most effective from the risk scenario. A player can draw up to five additional cards from the countermeasure card set if they cannot submit their card. A player does not have to submit a card if there are still no cards to submit.

Rule (2/2)

(8) Players rank the submitted cards in order of effect (affect) countermeasure through discussions between them.
(9) Players discuss the residual risks that are not able to protect with the submitted cards.
(10) Players repeat steps (3) to (9) three times.
* * * It can be changed to an arbitrary number of times although it is three times here. * * *

2. Recording
Players record the contents of the discussion on the worksheet.

Image of the game (1/4)

- Distribute threat and countermeasure cards to the players
- Present IoT · Attack Surface Card
- Submit the most serious threat card

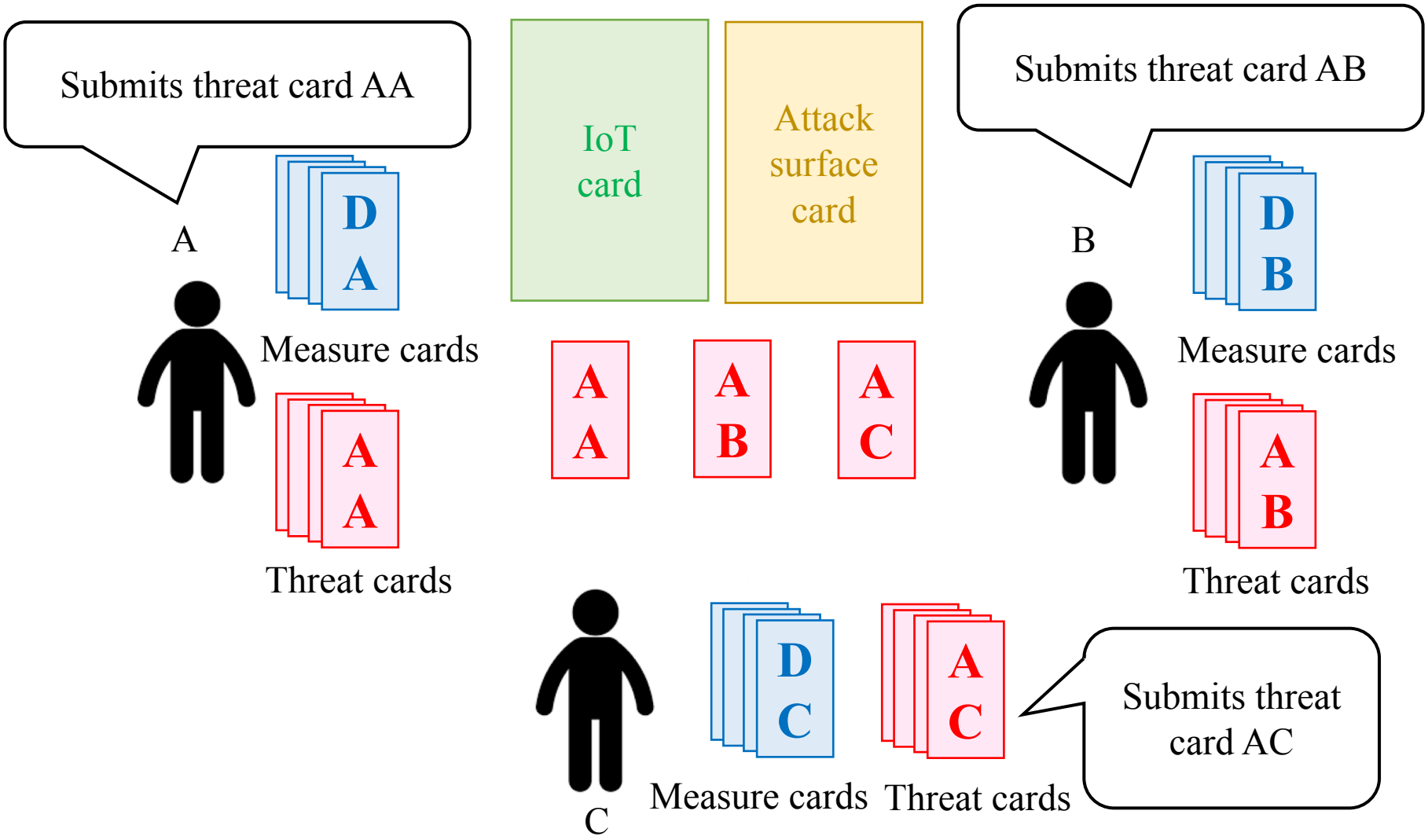

Image of the game (2/4)

- Rank threat cards in order of severity
- Describe the risk scenario

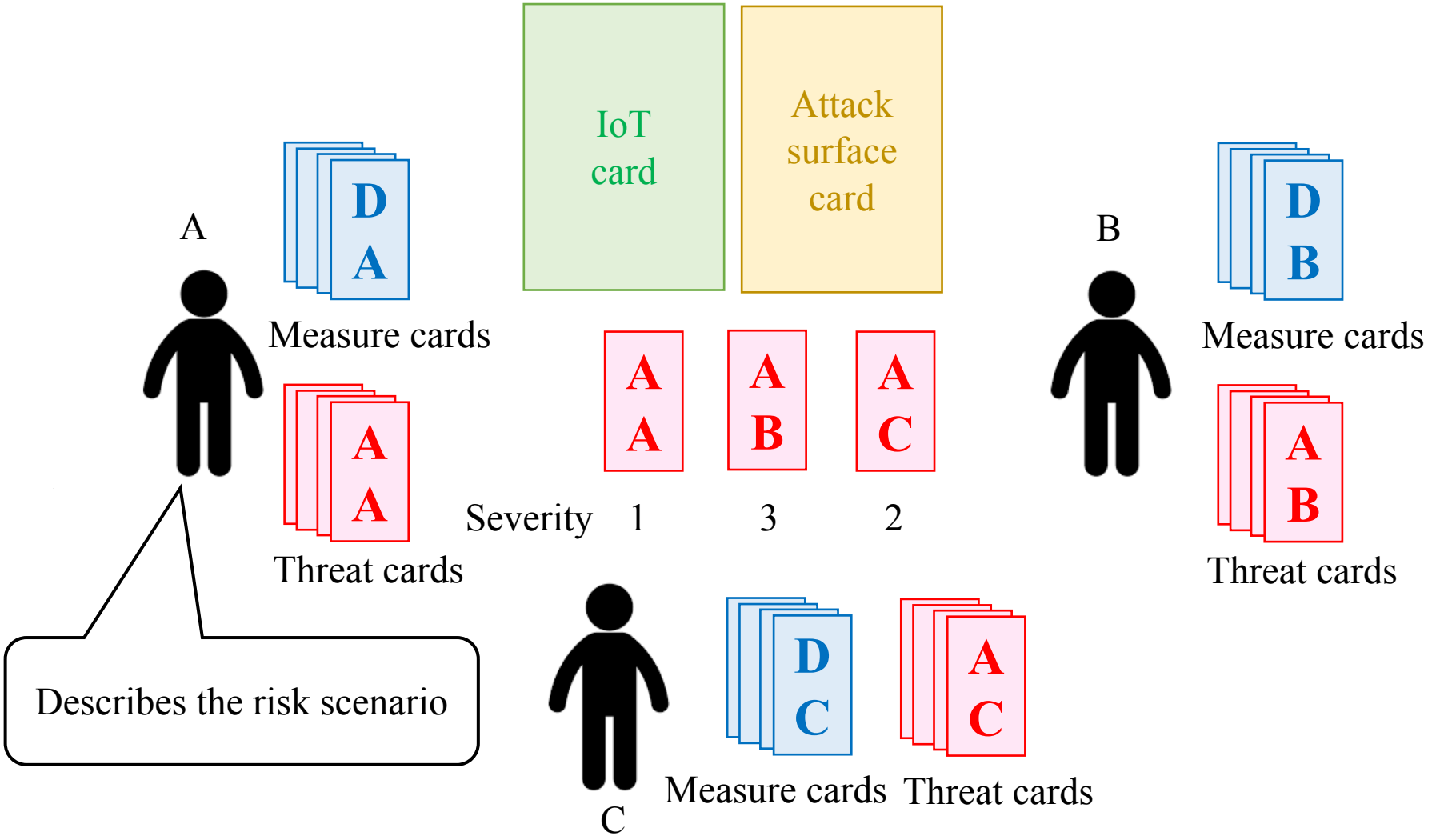

Image of the game (3/4)

- Submit the most effective countermeasure card

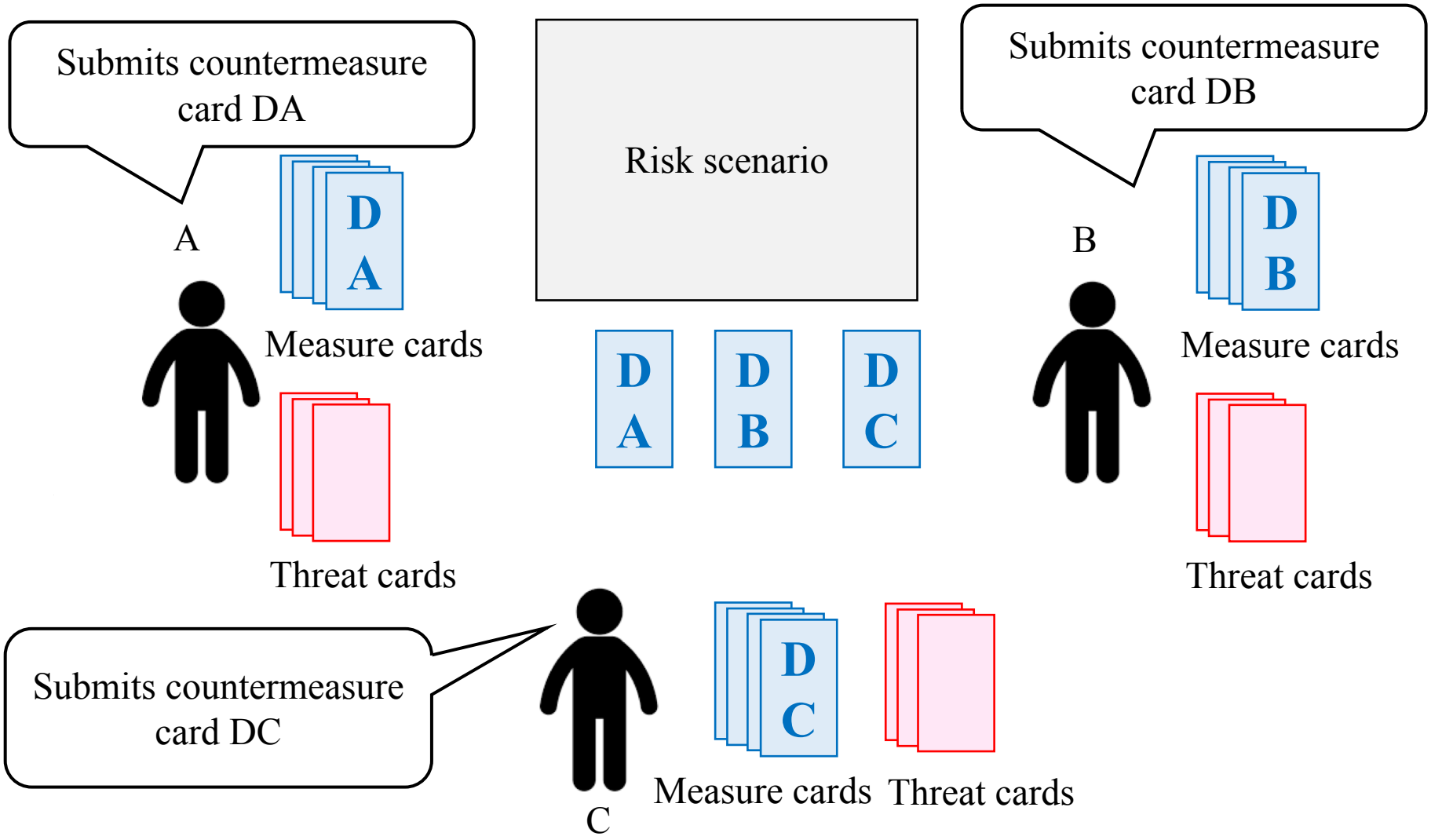

Image of the game (4/4)

- Rank countermeasures cards in order of effect
- Analysis of residual risk