ゲーム説明書	
プレイ人数	2～4 名
プレイ時間	30 分
対象者	新任 CSIRT 担当者

製作：ICSCoE 3 期生　CSIRT カードゲーム PJ

1. ゲームの目的

- インシデント発生時の本社 CSIRT 担当者と支社 CSIRT 担当者との連携の重要性を理解する。
- 本社 CSIRT 担当者、支社 CSIRT 担当者の行うべき役割を理解する。

2. コンポーネント

- **ゲームボード**
- **チップ([表]感染端末/[裏]マルウェア)**
  - -マルウェア A　：16 枚
  - -マルウェア B　：16 枚
  - -マルウェア C　：16 枚
- **担当者カード**
  - -本社 CSIRT 担当者　：1 枚
  - -北海道支社 CSIRT 担当者　：1 枚
  - -大阪支社 CSIRT 担当者　：1 枚
  - -博多支社 CSIRT 担当者　：1 枚
- **ネットワーク遮断カード**
  - -NW 遮断カード　：1 枚
- **役割紹介カード**
  - -本社 CSIRT 担当者　：1 枚
  - -北海道支社 CSIRT 担当者　：1 枚
  - -大阪支社 CSIRT 担当者　：1 枚
  - -博多支社 CSIRT 担当者　：1 枚
- **感染拡大カード**
  - -マルウェア感染(総務課)　：3 枚
  - -マルウェア感染(人事課)　：3 枚
  - -マルウェア感染(営業課)　：3 枚
  - -マルウェア横展開(北海道支社)　：3 枚
  - -マルウェア横展開(大阪支社)　：3 枚
  - -マルウェア横展開(博多支社)　：3 枚
  - -マルウェア感染拡大　：3 枚
  - -パンデミック　：2 枚
  - -感染拡大なし　：1 枚

チップ表側（感染端末）

チップ裏側（マルウェア）

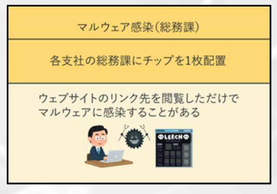
担当者カード

NW 遮断カード

役割紹介カード

感染拡大カード表側

感染拡大カード裏側



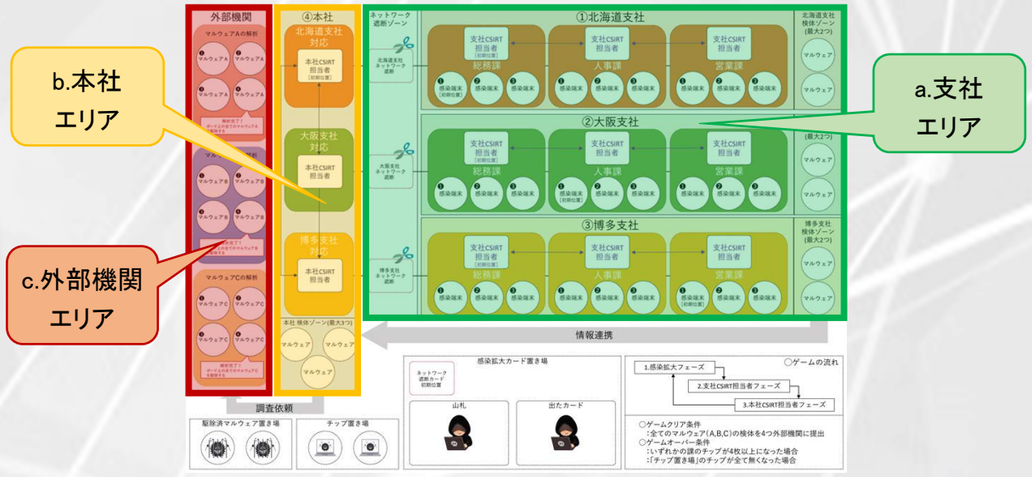
3. ストーリー

とある企業の各支社で標的型攻撃メールによる端末のマルウェア感染が発生した。本社 CSIRT 担当者、支社 CSIRT 担当者が協力して端末の隔離・解析を行い、マルウェアの感染拡大を防げ！

4. ゲームの準備

1. **役割の決定**
   まず、各プレイヤーの役割を決めます。役割は1.本社担当、2.北海道支社担当、3.大阪支社担当、4.博多支社担当があり、決定した担当者へ「役割紹介カード」を配布します。
   ※プレイ人数が少ない場合は、1人が複数の支社を担当します。
2. **ゲームボードの準備**
   ゲームボードは a.支社エリア、b.本社エリア、c.外部機関エリアに分かれています。

a.支社エリア	：3 つの支社に分かれており、各支社 CSIRT 担当者が作業を行います
b.本社エリア	：本社 CSIRT 担当者が作業を行います
c.外部機関エリア	：ここへマルウェアを移動させることがゲームクリアの条件となります



まず、準備として以下の通りにチップと各カードをゲームボードに配置します。

チップ	：シャッフル後、「チップ置き場」へ表向きに配置
感染拡大カード	：シャッフル後、「感染拡大カード置き場」山札へ表向きに配置
担当者カード(本社)	：本社の「北海道支社対応」マスへ配置
担当者カード(各支社)	：各支社の「総務課」マスへ配置
NW 遮断カード	：「ネットワーク遮断カード初期位置」マスへ配置

3. **チップの配置**
   ゲームスタート時には各支社にチップが 1 枚ずつ配置されます。チップを各支社の「感染端末チップ」マスのうち[初期位置]と書かれたマスへ配置します。

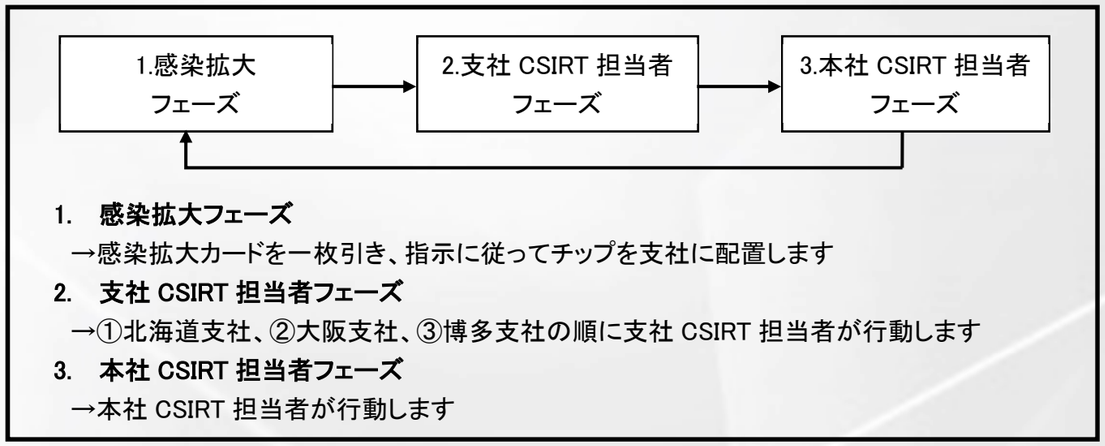
北海道支社	：チップを総務課の「感染端末」マスへ表向きに1つ配置
大阪支社	：チップを人事課の「感染端末」マスへ表向きに1つ配置
博多支社	：チップを営業課の「感染端末」マスへ表向きに1つ配置

5. ゲームの進め方

ゲームの流れ

プレーヤーはマルウェアの感染が拡大する前に、支社で感染端末を調査・隔離し、本社を経て外部機関(セキュリティベンダー)に送ります。外部機関では送付されたマルウェアを解析することでマルウェア駆除のプログラムを作成し、支社のマルウェアが駆除できるようになります。

ゲームは以下の 3 つのフェーズを繰り返すことで進行していきます。

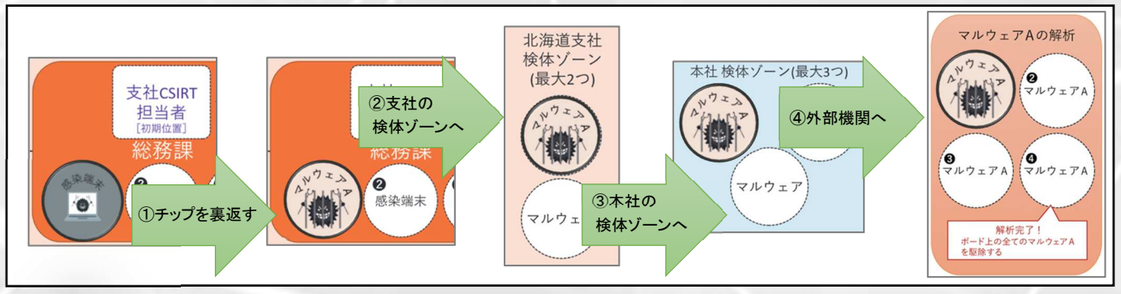


1. **感染拡大フェーズ**
   →感染拡大カードを一枚引き、指示に従ってチップを支社に配置します
2. **支社 CSIRT 担当者フェーズ**
   →①北海道支社、②大阪支社、③博多支社の順に支社 CSIRT 担当者が行動します
3. **本社 CSIRT 担当者フェーズ**
   →本社 CSIRT 担当者が行動します

チップ(マルウェア)の流れ

チップは以下の①～④の支社担当者及び本社担当者の行動により、支社から本社を経て外部機関に提出されます。いずれかの支社の課にチップが 4 つ配置される前に、外部機関に3種類(A,B,C)のマルウェアを 4 つずつ送ることができればゲームクリアとなります。

支社担当者/本社担当者の行動	実施者	チップの動き
①端末調査/端末隔離	支社担当者	チップを裏返す(マルウェアの種類が判明)
②感染端末からマルウェア検体の回収	支社担当者	チップを[支社の各課]→[支社　検体ゾーン]へ移動
③本社 CSIRT への情報連携	支社担当者	チップを[支社　検体ゾーン]→[本社　検体ゾーン]へ移動
④外部機関へマルウェア検体調査依頼	本社担当者	チップを[本社　検体ゾーン]→[外部機関]へ移動



- 外部機関で同じマルウェアが 4 つ揃うと、ボード上の同じマルウェアを駆除することができます
- 支社/本社の検体ゾーンに空きがなければ、そこへチップを移動させることはできません

ネットワーク遮断について

支社のチップ配置状況から止むを得ないと判断した場合、本社担当者はいずれかの支社の NW 遮断を行うことができます。NW 遮断された支社には、以降チップが配置されませんが、その支社担当者は次のターン以降に作業を行うことができず、また、NW 遮断対応のため本社担当者も次のターンは1回休みとなります。

プレイヤーの役割

支社 CSIRT 担当者
支社内を移動し、感染端末の調査・隔離や本社担当者への情報連携を行います。
以下の【行動1】→【行動2】の順で作業を行うことができます。

【行動 1】	1つ隣の課への移動が可能(その場に留まっても良い)
【行動 2】	各ターンにおいて、以下のいずれかの作業を1つだけ実施可能 ① **端末調査/端末隔離** →この課の全てのチップ(感染端末)を裏返す ② **感染端末からマルウェア検体の回収** →この課の 1 枚のマルウェアを[支社　検体ゾーン]へ移動させる ③ **本社 CSIRT への情報連携** →当該支社の[支社　検体ゾーン]にある全てのマルウェアを[本社　検体ゾーン]へ移動させる

本社 CSIRT 担当者
本社内を移動し、支社の支援や外部機関との連携を行います。
以下の【行動1】→【行動2】の順で作業を行うことができます。

【行動 1】	別の支社対応マスへの移動が可能(その場に留まっても良い)
【行動 2】	各ターンにおいて、以下のいずれかの作業を1つだけ実施可能 ① **セキュリティ会社へマルウェア調査依頼** →対応している支社の全てのチップ(感染端末)を裏返す ② **外部機関へマルウェア検体調査依頼** →[本社　検体ゾーン]の全てのマルウェアを[外部機関]へ移動させる ③ **いずれかの支社のネットワーク遮断(※1度のみ利用可能)** →ネットワーク遮断ゾーンのいずれかの支社のマスに「NW 遮断カード」を配置する。**(本社担当者は次のターン一回休み)** ※ネットワーク遮断を行った支社は、今後チップが配置されない。

6. 勝利条件

全てのマルウェア(A,B,C)の検体を 4 つ外部機関に提出すればゲームクリアとなります。
逆に、以下のいずれかの状態になった場合は、ゲームオーバとなります。

- いずれかの課のチップが 4 枚以上になった場合
- 「チップ置き場」のチップが全て無くなった場合