MALWARE CONTAINMENT

説明書		
プレイ人数	プレイヤー	4～5人
	進行役	1人
プレイ時間	30分 ～ 60分	

コンポーネント

【内容物】

- ゲームボード
- 役職カード
  - コマンダー 1枚
  - フォレンジックエンジニア 1枚
  - リサーチャー 1枚
  - ノーティフィケーション 2枚
- 端末カード
  - 遠隔操作マルウェア 2枚
  - スパイウェア 1枚
  - ランサムウェア 1枚
  - 正常な端末 2枚
- イベントカード
  - 相談に乗ってほしい 1枚
  - 製品設定のお願い 1枚
  - 差し入れ 2枚

【別途用意する物】

- ゲームメモ 各自
- 筆記用具 各自
- ポストイット 1部
- ストップウォッチ（3分計測用） 1個

ストーリー

組織の端末がマルウエア（= コンピュータウィルス）に感染した!?
専門家の持つ能力を駆使して、感染している端末を見つけ出せ!!

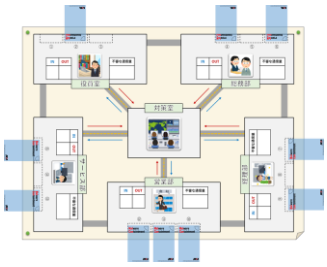
コンピュータセキュリティに関する問題に対応するため、専門家により結成されたチーム（CSIRT：シーサート）に、お客様サポートセンターから電話がかかってきた。

「お客様より、うちから不審なメールが来たと連絡がありました」

事実確認を行ったがどうやら組織内の端末のどれかが、外部から遠隔操作されているらしい。チームメンバーはそれぞれの専門性を活かしながら、マルウエアに感染した端末の捜査を開始する。

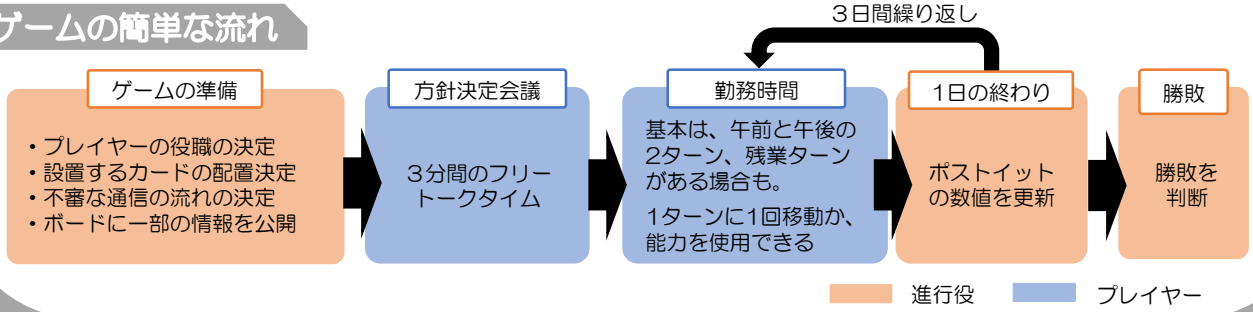
3日後には、お客様に対する説明会を実施しなければならない。それまでに CSIRT チームは、マルウエアに感染した端末を特定し端末を封じ込めることができるのか…

ゲームの目的



本ゲームは、参加者が進行役とプレイヤーに分かれてプレイします。
進行役は、ゲームボード上に設置するカードと、カードから発信される不審な通信の流れを決めます。ゲームの流れに応じて情報が変化するため、その情報を管理し、ゲーム全体の進行を務めます。
プレイヤーは CSIRT として配布された役職カードの持つ能力を駆使し、ゲームボード上に設置された端末カードをめくったり、マルウェアに感染した端末を封じ込めることを目指します。

ゲームの簡単な流れ



まずテーブル上にゲームボードを置き、ゲームメモと筆記用具を全員の手元に用意します。続いて進行役は、プレイヤーにランダムにカードを配り、役職を決定します。プレイヤーの人数に応じて「ノーティフィケーション」のカードを増減させ、配布してください。

役職カードについて

それぞれの役職には、それぞれ異なった能力があります。能力は、ゲーム中の「勤務時間」で使用することができます。複数の能力がある場合は、１回に１つだけ使用することができます。

- **コマンダー**（勤務時間：午前/午後）
このプレイヤーは、業務時間中でも、発言できる（別プレイヤーとの会話は不可）

●能力
①１日に 1回だけ、指定したプレイヤー １名に残業ターンを１回付与する
（ノーティフィケーションを指定した場合、全員の残業ターンが終わった後に
もう一度指定されたプレイヤーの残業ターンが始まります）
②フォレンジックエンジニア、リサーチャーの能力を使用できる

- **リサーチャー**（勤務時間：午前/午後）

●能力
①自身のいる部署と対策室の間の通信量及びその通信の向きが(自分だけ)わかる
②自身がいる部署のどのカードがイベントカードなのか(自分だけ)わかる

- **フォレンジックエンジニア**（勤務時間：午前/午後）

●能力
自身がいる部署の指定したカードを１枚めくり、カードを(自分だけ)確認することができる（イベントカードだった場合、その効果が発動する）

- **ノーティフィケーション**（勤務時間：午前/午後/残業）
このプレイヤーは、勤務時間において残業ターンまで行動することができる

●能力
自身のいる部署のカード１枚を全体に公開することでカードを封じ込める事ができる
（イベントカードや正常な端末カードだった場合、敗北となる）

端末カード、イベントカードについて

続いて進行役は、ゲームボード上に設置する端末カード、イベントカードの配置を決定し、自身のゲームメモに記載します。端末カード、イベントカードは全部で 10枚あり、各部署に必ず １枚は設置する必要があります。決定したらカードの詳細がわからないよう裏向きで設置します。

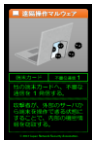
■ 端末カードの種類 ■（全 ６ 枚）

端末カードには、不審な通信量を持つカードがあります。ノーティフィケーションによって、不審な通信を持つカードが封じ込められた時点で、不審な通信は無くなります。

- ランサムウェア（全1枚）
◆ 不審な通信：1

- スパイウェア（全1枚）
◆ 不審な通信：2

- 正常な端末（全２枚）
◆ 不審な通信：0



- 遠隔操作マルウェア（全２枚）
◆ 不審な通信：1
このカードから発信される不審な通信は対策室を通って、別の端末カードへ向かう。その部署の不審な通信量の総量を +1 する

■ イベントカードの種類 ■ (全 4 枚)

イベントカードには、不審な通信量を持つカードがあります。また、イベントカードには特別な効果を持つカードもあり、フォレンジックエンジニアやコマンダーによってめくられた際に、効果が発生します。（ノーティフィケーションによってめくられた場合、プレイヤーの敗北となるため、効果は発生しません）効果は発生した際に全員に伝えられ、めくったカードは封じ込められます

- 相談に乗ってほしい (全１枚)

◆ 不審な通信：1

このカードをめくったプレイヤーは、次の勤務ターン１回が休みとなる

- 設定変更の依頼 (全１枚)

◆ 不審な通信：1

このカードをめくった場合、ゲームクリアまでに、リサーチャーもしくはコマンダーをこの部屋まで向かわせなければならない。向かわせることができなかった場合、プレイヤーの敗北となる

- 差し入れ (全２枚)

◆ 不審な通信：0

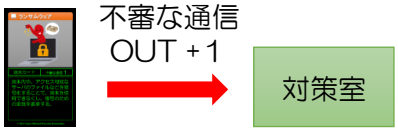
このカードをめくったプレイヤーは、そのターンに追加で２回行動できる

不審な通信について

端末カード、イベントカードからは「不審な通信」が別の部署やカードに流れています。不審な通信には２種類あり、対策室で通信が止められるものと、対策室を経由して、端末カードに通信するものがあります。

■ 対策室で止められる不審な通信の流れ（右図の赤矢印）

遠隔操作マルウェア以外のカードが発信する不審な通信がこれにあたります。端末カードから対策室に対して、OUT の通信が発生します。



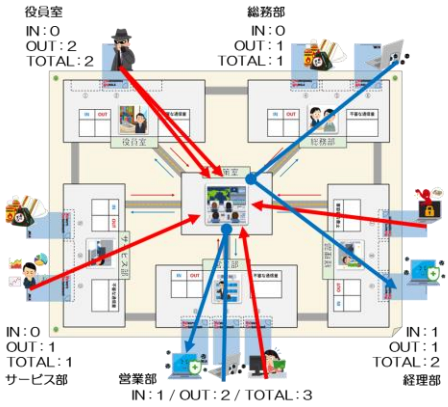
■ 端末カードに通信する不審な通信の流れ（右図の青矢印）

遠隔操作マルウェアが発信する不審な通信がこれにあたります。端末カードから対策室に対して、OUT の通信が発生し、対策室から別の端末カードに IN の通信が発生します。１つの端末カードに複数の通信（IN）が発生してしまっても問題ない。

■ ボードに記載された不審な通信量(TOTAL)について

ゲームボード上の各部署に記載されている不正な通信量は、その部署の端末カードに関する IN と OUT の数値を合算したものになります。ゲーム中は、TOTAL の通信量が各部署のポストイットにその数値が示されており、プレイヤーは常にこの数値を確認することができます。

また、この数値が封じ込めによって変化した場合、その数値は１日の終わりに更新されます。



カードの設置例と
不審な通信の流れの例

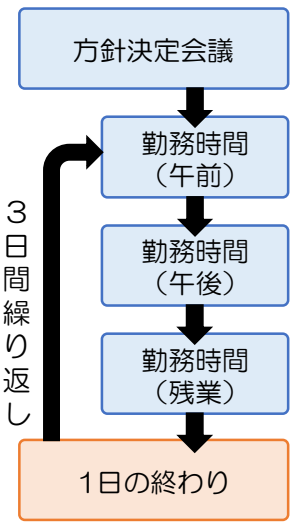
カードの封じ込め時の処理について

不審な通信を持つカードが封じこめられた場合、発生していた通信はその時点で消滅します。

また、遠隔操作マルウェアの通信先として指定されていた端末カードが封じ込められた場合も不正な通信は消滅します。しかし、勝利条件をみたすには、別途遠隔操作マルウェアカードを封じ込める必要があります。

ゲームの流れ

進行役がボードにカードを設置し、不審な通信量を記載したら、ゲームが開始されます。
CSIRT は、まず対策室に集合し、「方針決定会議」を行って今後の調査方針などを相談します。その後、３日間の「勤務時間」で各部署を移動したり、能力を使用したりして、2枚の遠隔操作マルウェアカードを封じ込めることが CSIRT の勝利条件となります。



CSIRT は、各プレイヤーの能力を再確認したり、どのプレイヤーが、どの部署に行くか等を自由に話し合うことができます。

CSIRT は、各勤務時間に、2種類の行動のどちらかを選んで１回だけ実行することができます。

- ◆ 部署を移動する
  隣り合う部署へ１回移動できます。
- ◆ 能力を使う
  役職カードの能力を使用できます。

行動順は、コマンダーから時計回りになります。勤務時間の間、コマンダー以外のプレイヤーは発言することができません。しかし、同じ部署にいるプレイヤーとはゲームメモを交換することができます。

進行役は CSIRT の行動に応じて、変化した不審な通信を再計算し、変化がある場合は、ポストイットの数値を更新します。

また、３日間の間に１回だけ、コマンダーの判断で、ターンの消費なしに「方針決定会議」と同様に３分間の間だけ自由に話し合うことのできる「特別会議」を開催することができます。この場合、プレイヤーは各自がいまいる部署から移動せずに話し合いを行います。

ゲームの勝敗

3日目に予定されていた勤務時間が全て終了した時点、もしくは敗北条件を１つでも満たした場合に勝敗の判定が行われます。

【勝利条件】
- 端末カード「遠隔操作マルウェア」が２枚とも封じ込められている

【敗北条件】
- 端末カード「遠隔操作マルウェア」が２枚とも封じ込められていない
- イベントカード「設定変更の依頼」の効果を達成できていない
- ノーティフィケーションが端末カード「正常な端末」もしくはイベントカードを封じ込めてしまう

提供

ゲームデザイン	JNSA　教育部会　ゲーム教育PJ　（青木 翔） http://www.jnsa.org/edu/secgame/
イラスト素材	いらすとや（@irasutoya）
Publisher	NPO法人　日本ネットワークセキュリティ協会（JNSA）
協力	一般社団法人 JPCERT コーディネーションセンター

▼ JNSA 教育部会 ゲーム教育PJ ゲーム第一弾 「セキュリティ専門家 人狼」も発売中！

JNSA ゲーム教育プロジェクト

情報セキュリティ分野におけるゲーム教育の企画・推進を行っています。ゲームを活用した振り返り教育の普及・促進を図るため、イベントの企画や、実施を行っています。

本団体は、非営利団体であり、購入に必要な金額は実費分だけを頂いています。

@jnsa　/jnsagame