MALWARE CONTAINMENT Instruction Paper

① 役職の決定

皆さんは、今年度からセキュリティインシデントに対応する組織CSIRT(シーサート)に所属することになりました。
それぞれの役職は、ファシリテータよりランダムに配られる役職カードによって決定されます。

② 赴任先の確認(内容物の確認)

まず皆さんは、現状存在しているものと、今後の対応に必要であると言われたものがあるかどうかを確認することにしました。
※ カードの内訳については、付属の説明書またはゲームメモを参照してください。

▷ 現状存在しているもの

- **ゲームボード**
- **役職カード (5枚)**
- **端末カード (6枚)**
- **イベントカード (4枚)**
- **プレイヤー用ゲームメモ (人数分)**

▷ 今後の対応に必要なもの

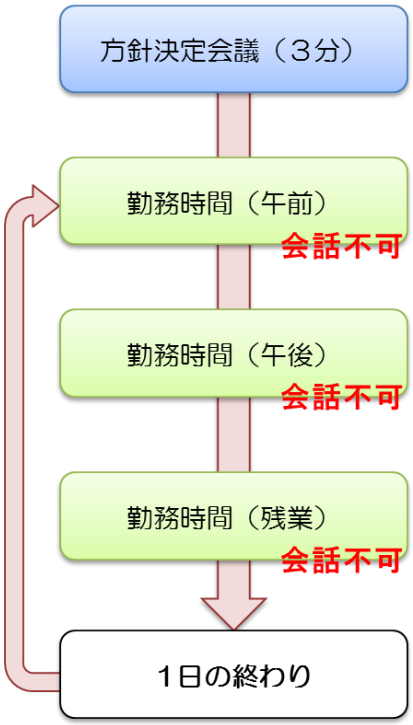
- **筆記用具**
- **ポストイット**
- **時間を測定できるもの (3分目安を確認できれば良い)**

MALWARE CONTAINMENT

Instruction Paper

③ 過去の対応経験の確認(ゲームの説明)

続いて、過去にインシデントが発生した際の対応が記録されていたので、どのような業務を行うのか皆さんは確認することにしました。**どうやら組織内の端末に遠隔操作マルウェアが侵入していることが確認され、端末の調査をしていたようです。**



③-1. 行動の流れ

まず初めに、CSIRT全員は「特別対策室」に集合し、全体の行動方針を相談していたようです。

基本的に**業務が出来るのは、「午前」と「午後」の勤務時間のみ**
残業が出来るのは、コマンダーより残業指示が出た従業員のみ

各勤務時間では、以下のうちの一種類を選んで行動することしかできない

- **現在居る部屋で待機する**
- **隣り合う部屋に移動する**
- **役職が持つ能力を”どれか一種類のみ”使用する**

なお、インシデントが社内に広く知れ渡ると混乱を招くため、**勤務時間中は、会話ができなかった**ようです。そのため、**同じ部屋にいるメンバと結果を記したメモを交換し、お互いに書き写して情報交換**をしていました

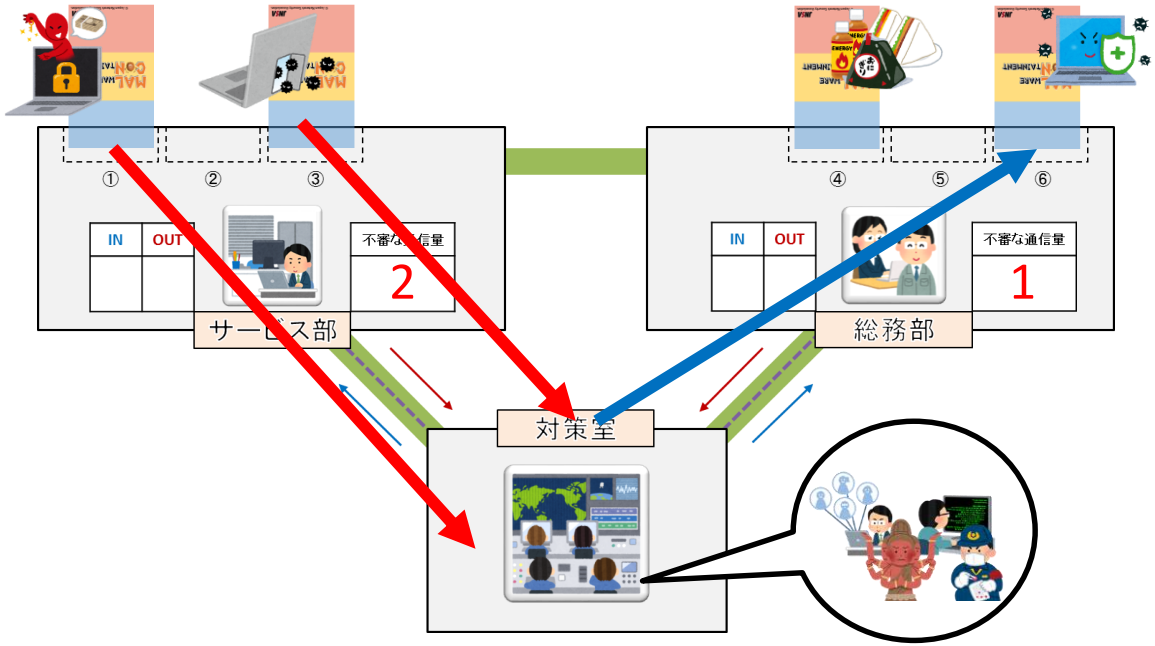
MALWARE CONTAINMENT

Instruction Paper

③-2. 社内の端末調査

当時は、現在の特別対策室と、総務部、サービス部の2つの部署に端末が4台しか無かったようです。
現在は、特別対策室と５つの部署があり、端末は全部で10台あります。

調査を始める前に、当時のCSIRTは各部署の通信量に着目しました。（下図 赤字の数字）
この会社では、端末から発せられる不審な通信を記録しているため、マルウェアに感染している端末を推測することが可能です。(各カードの持つ不審な通信量は後述します)



不審な通信について

端末が持つ不審な通信は、基本対策室を経由して外部へと通信を行います。(①のカード参照)

しかし、遠隔操作マルウェアに感染した端末は、対策室を経由し他の端末カードへ通信を行う。(②、④のカード参照)

各部署に記載されている通信量はその部署から対策室への通信と、対策室から部署への通信を合算した数値になります。

MALWARE CONTAINMENT

Instruction Paper

③-3. 端末・イベントについて

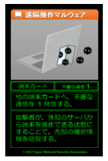
場に伏せてあるカードには端末カードだけでなく、イベントカードも存在した。
イベントカードは、役職の能力を使って調査(後述)すると同時にイベントが発生したようだ。

端末カード

■ランサムウェア（1枚）
- 不審な通信 1

■正常な端末（2枚）
- 不審な通信 0

■スパイウェア（1枚）
- 不審な通信 2



■遠隔操作マルウェア（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

■相談に乗ってほしい（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

■差し入れ（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

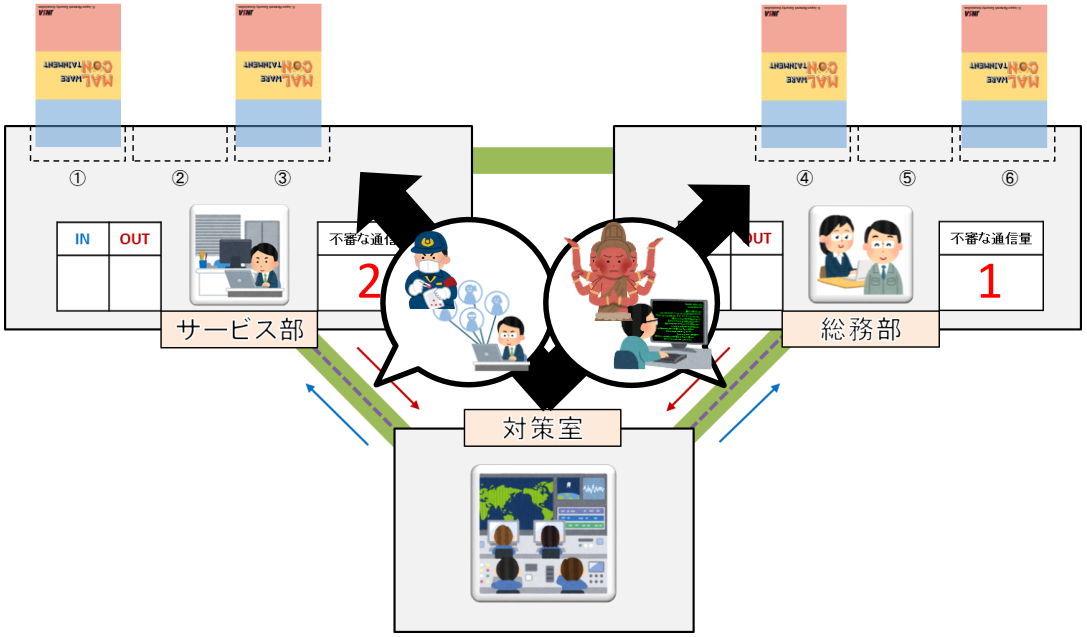
■製品設定のお願い（1枚）
- 不審な通信 1
  このカードをめくった場合、ゲームクリアまでに、リサーチャーもしくはコマンダーをこの部屋まで向かわせなければならない。向かわせることができなかった場合、プレイヤーの敗北となる

MALWARE CONTAINMENT

Instruction Paper

③-4. 捜査の開始

CSIRTは午前の勤務時間で、二手に分かれて移動した。
そして、午後の勤務時間を使い、以下のような調査を行った。
(役職が持つ能力は、次のページで説明します。)



【午後の行動とその結果】

コマンダー
カード④を確認する

⇒ 差し入れ
勤務時間(残業)獲得

リサーチャー
総務部と対策室を走る
通信の向きを確認する

ノーティフィケーション
待機

フォレンジックエンジニア
カード③を確認する

MALWARE CONTAINMENT

Instruction Paper

③-5. 役職ごとの能力

■コマンダー

業務時間中でも、発言できる（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

◆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

◆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

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）

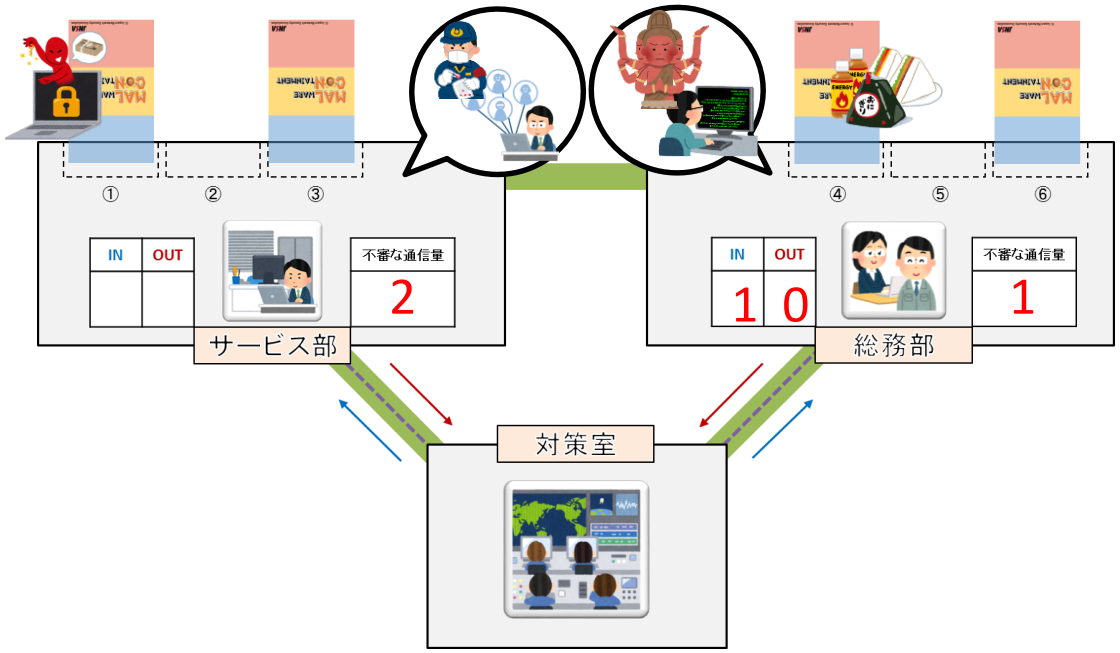
MALWARE CONTAINMENT

Instruction Paper

③-6. 封じ込め

コマンダーはリサーチャーと情報を共有し、総務部に感染端末が無いことを突き止めました。
そのため、フォレンジックエンジニアの調査回数を増やすため、残業を指示した。

残業時間にフォレンジックエンジニアにカード③を確認し、遠隔操作されている端末を発見。
ノーティフィケーションの封じ込め能力で無事、今回のインシデントが収束した…



【残業の行動と結果】

コマンダー
フォレンジックエンジニアへ残業を付与

リサーチャー
退勤

ノーティフィケーション
カード③の封じ込め

フォレンジックエンジニア
カード③を確認する

MALWARE CONTAINMENT

Instruction Paper

④ ゲームの開始

貴方の組織の端末から、不審な通信が発生しています。

ようやく業務を理解したところで、セキュリティの専門組織から
組織内の端末に関する情報を受け取りました。
以前の被害を受けてか、対応を急いだ経営陣は顧客説明会の連絡
を流してしまいました！まだ事実確認もできていないのに！

CSIRT に課せられた使命は、
不正に操作されている端末を見つけ出し、影響が無いよう封じ込めること。

情報によると、遠隔操作マルウェアに感染している恐れのある端末は**2台**のようです。
新人CSIRTの皆さんは封じ込めを成功させ、この事態を乗り越えることができるのか!?

⑤ ゲームの勝敗

顧客説明会の実施は、4日後。つまり3日間で全ての遠隔操作マルウェアが封じ込められている必要があります。また、ある条件を満たせていない場合は敗北となります。

■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

CSIRT チームの勝利となります

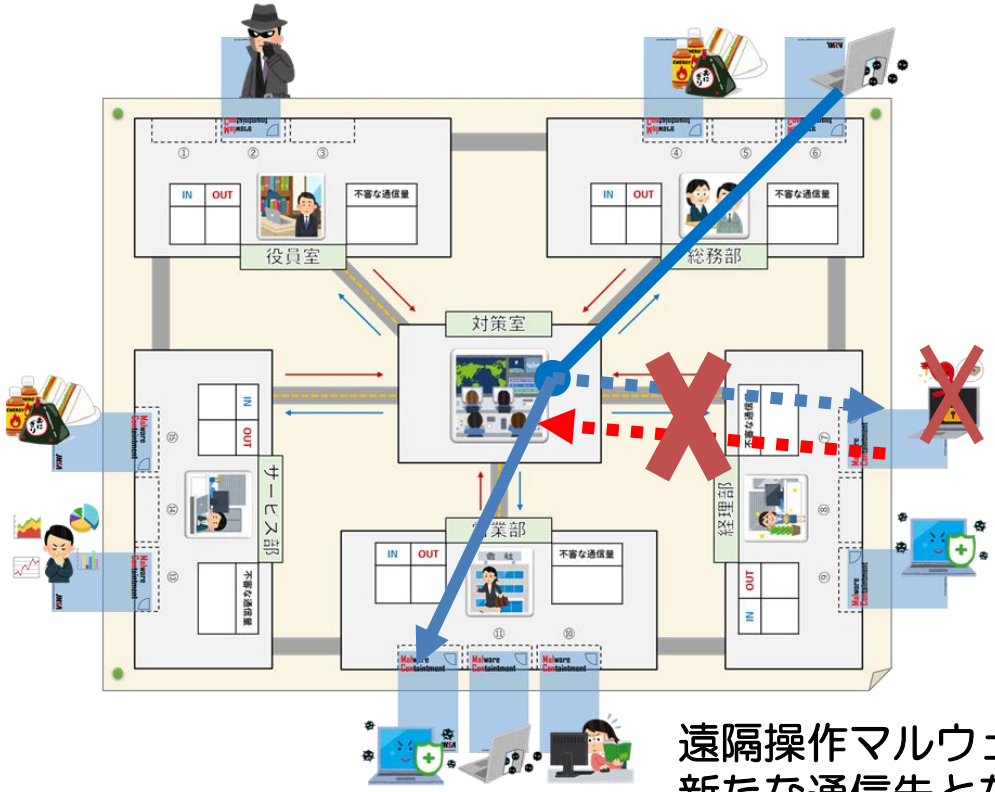
■端末カード「遠隔操作マルウェア」が２枚とも封じ込められていない
■イベントカード「設定変更の依頼」の効果が発動していて、達成できていない
■ノーティフィケーションが端末カード「正常な端末」もしくはイベントカードを封じ込めてしまう

CSIRT チームの敗北となります

敗北してしまった場合は、調査代表者として
謝罪会見に呼ばれてしまうかもしれません…!!

補足

- 遠隔操作マルウェアの通信先は端末カードのみです
- 通信先のカードが封じ込められた場合は、別の端末カードに通信先が変化します（通信量も変化します）



ランサムウェアが封じ込められる
→ ランサムウェアの通信： -1
→ 通信先でなくなる　　： -1
不審な通信量は -2 される

遠隔操作マルウェアの
新たな通信先となる +1

MALWARE CONTAINMENT

方針決定会議

- この時間は全員が発言できます。
- プレイヤーは全員、対策室にいます。

【進行のためのヒント】

- 各部署の不正な通信量の数値と、配置されたカードからどこにどんな通信量のカードがあるか想定する
- どの役職がどこに行くのか方針を決める
- 「特別会議」をいつ行うか決めておく

MALWARE CONTAINMENT

１日目 – 勤務時間（午前）

- コマンダーしか発言できません。
- 出来るだけ顔色を抑えて下さい。
- コマンダーから時計周りの順番です

【各人ができること】

部署の移動

能力の使用

MALWARE CONTAINMENT

１日目 – 勤務時間（午後）

- コマンダーしか発言できません。
- 出来るだけ顔色を抑えて下さい。
- コマンダーから時計周りの順番です

【情報共有の仕方】

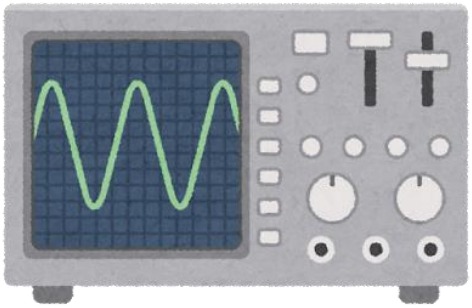
同じ部屋にいるメンバーとは、
メモだけを交換することができます。
喋ることはコマンダー以外不可能です。

MALWARE CONTAINMENT

１日目 – 勤務時間（残業）

- コマンダーしか発言できません。
- 出来るだけ顔色を抑えて下さい。
- コマンダーから時計周りの順番です

【不審な通信量の変化】



端末カードの封じ込めや、イベントカードの調査を行った場合は、１日の終わりにボード上に記載の通信量が変化します。

MALWARE CONTAINMENT

２日目 – 勤務時間（午前）

- コマンダーしか発言できません。
- 出来るだけ顔色を抑えて下さい。
- コマンダーから時計周りの順番です

【各人ができること】

部署の移動

能力の使用

MALWARE CONTAINMENT

２日目 – 勤務時間（午後）

- コマンダーしか発言できません。
- 出来るだけ顔色を抑えて下さい。
- コマンダーから時計周りの順番です

【各人ができること】

部署の移動

能力の使用

MALWARE CONTAINMENT

２日目 – 勤務時間（残業）

・コマンダーしか発言できません。
・出来るだけ顔色を抑えて下さい。
・コマンダーから時計周りの順番です

【各人ができること】

部署の移動

能力の使用

MALWARE CONTAINMENT

３日目 – 勤務時間（午前）

・コマンダーしか発言できません。
・出来るだけ顔色を抑えて下さい。
・コマンダーから時計周りの順番です

【情報の整理】

共有できていない情報があり、ターンが限られている場合、
特別会議を開くのも１つの方法です。

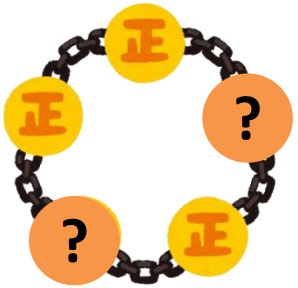
MALWARE CONTAINMENT

３日目 – 勤務時間（午後）

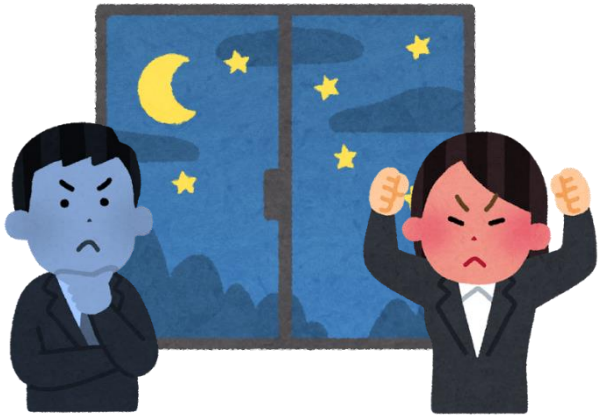
・コマンダーしか発言できません。
・出来るだけ顔色を抑えて下さい。
・コマンダーから時計周りの順番です

【ゲームに勝利できていない場合】

最終ターンで、ノーティフィケーションが「賭ける」場合に備え、可能な限り正確な情報を増やしておきましょう。



MALWARE CONTAINMENT



３日目 – 勤務時間（残業）

・コマンダーしか発言できません。
・出来るだけ顔色を抑えて下さい。
・コマンダーから時計周りの順番です

TIME UP!!

CLEAR

／

GAME OVER

MALWARE CONTAINMENT

顧客説明会

ゲームを振り返って以下のような事を考えてみましょう。

勝利の鍵となった行動

後悔していること

同様の状況に備えた改善策

MVP