セキュリティ専門家 人狼

特定非営利活動法人
日本ネットワークセキュリティ協会
Japan Network Security Association

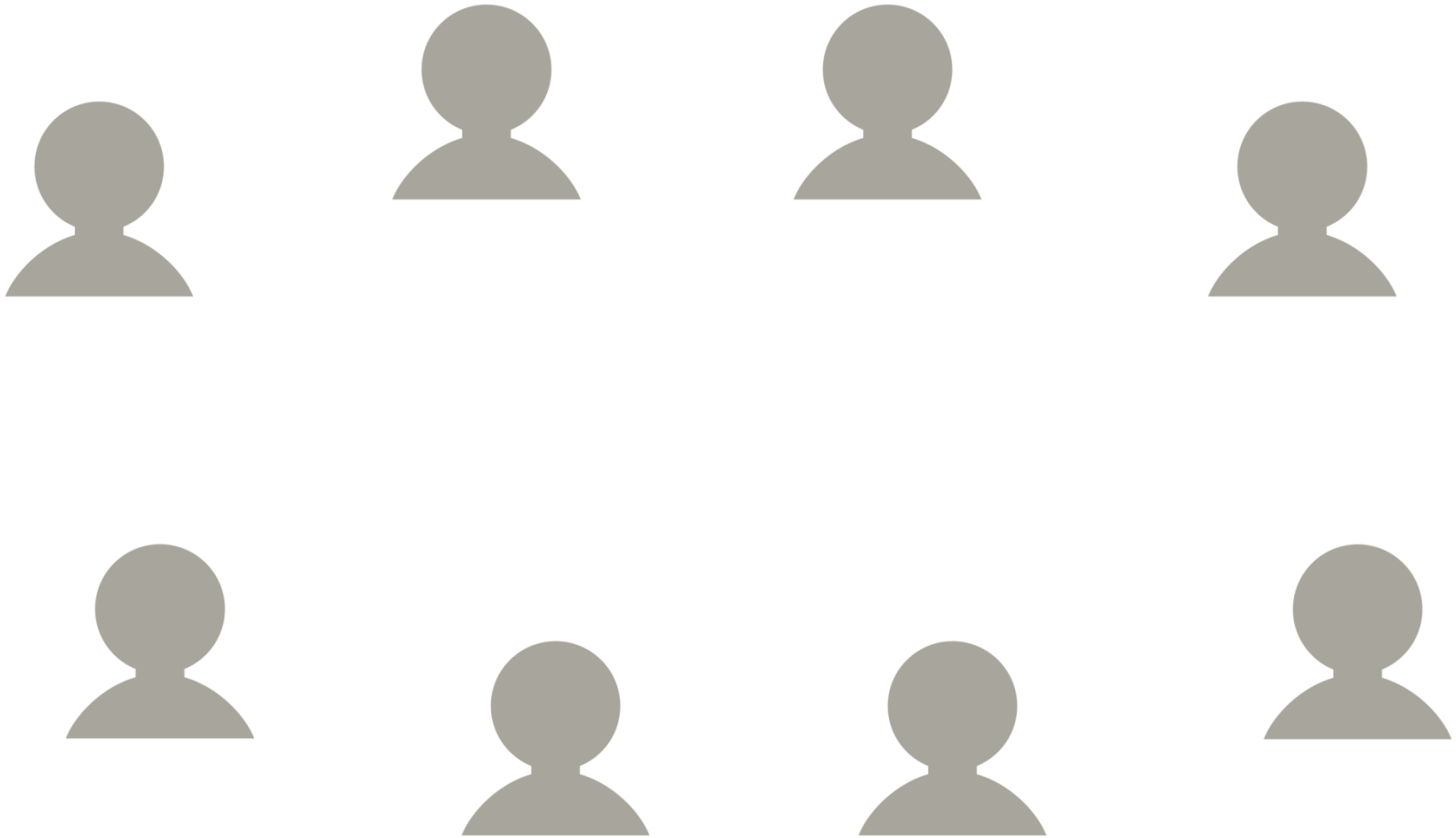
教育部会 ゲーム教育Project
Noriaki HAYASHI

インスト（ルール説明）

ゲームグループを作る

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- 円になる形でゲームグループを作る。



役職カードを配る

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- 役職カードは1人1枚。

役職カードを確認

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

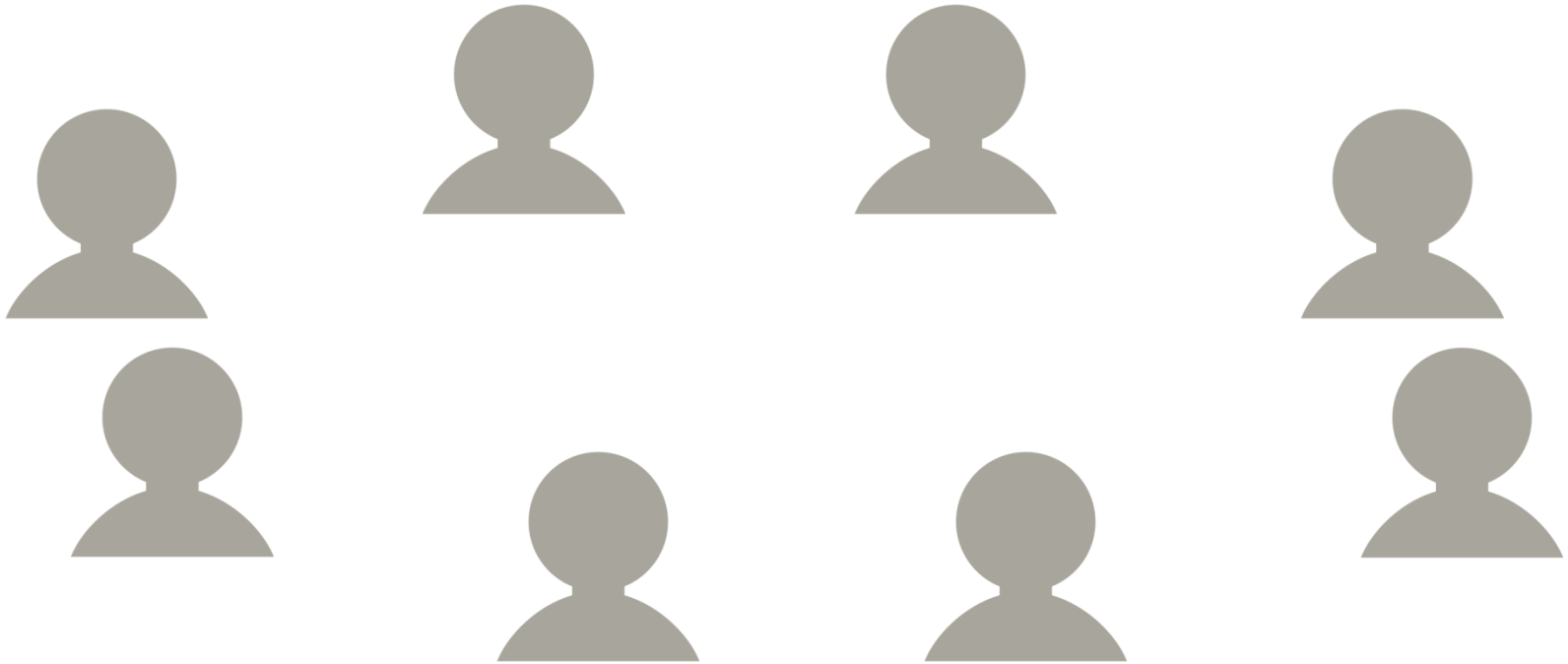
- 周りの人に役職を明かさず確認する。

自分のカードを確認したら
役職を他の参加者に明かさないよう伏せておく。

不正調査：被疑者面接

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

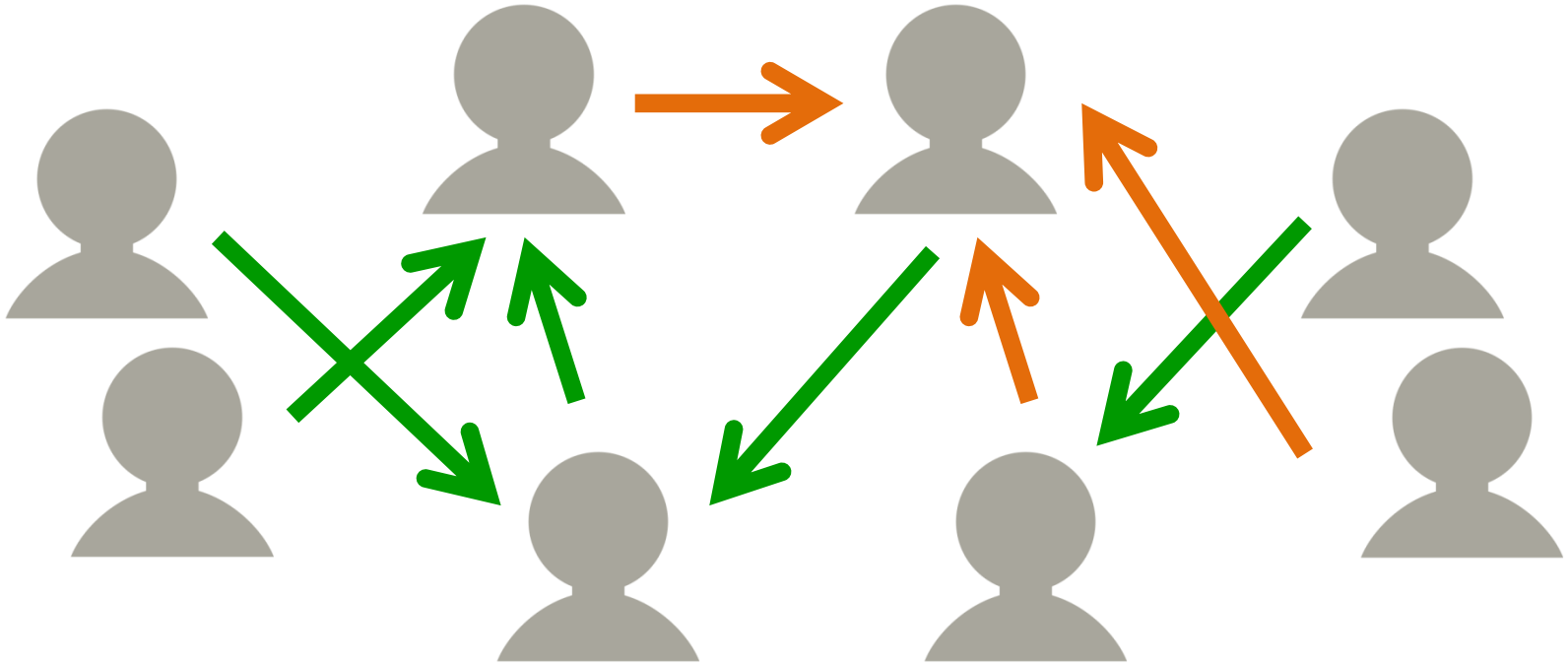
- シーサート陣営は**処遇に不満**を抱えた汚職者を面接によって推定する。
- 汚職者は怪しまれないように話合いに参加。



不正調査：解雇者の決定

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

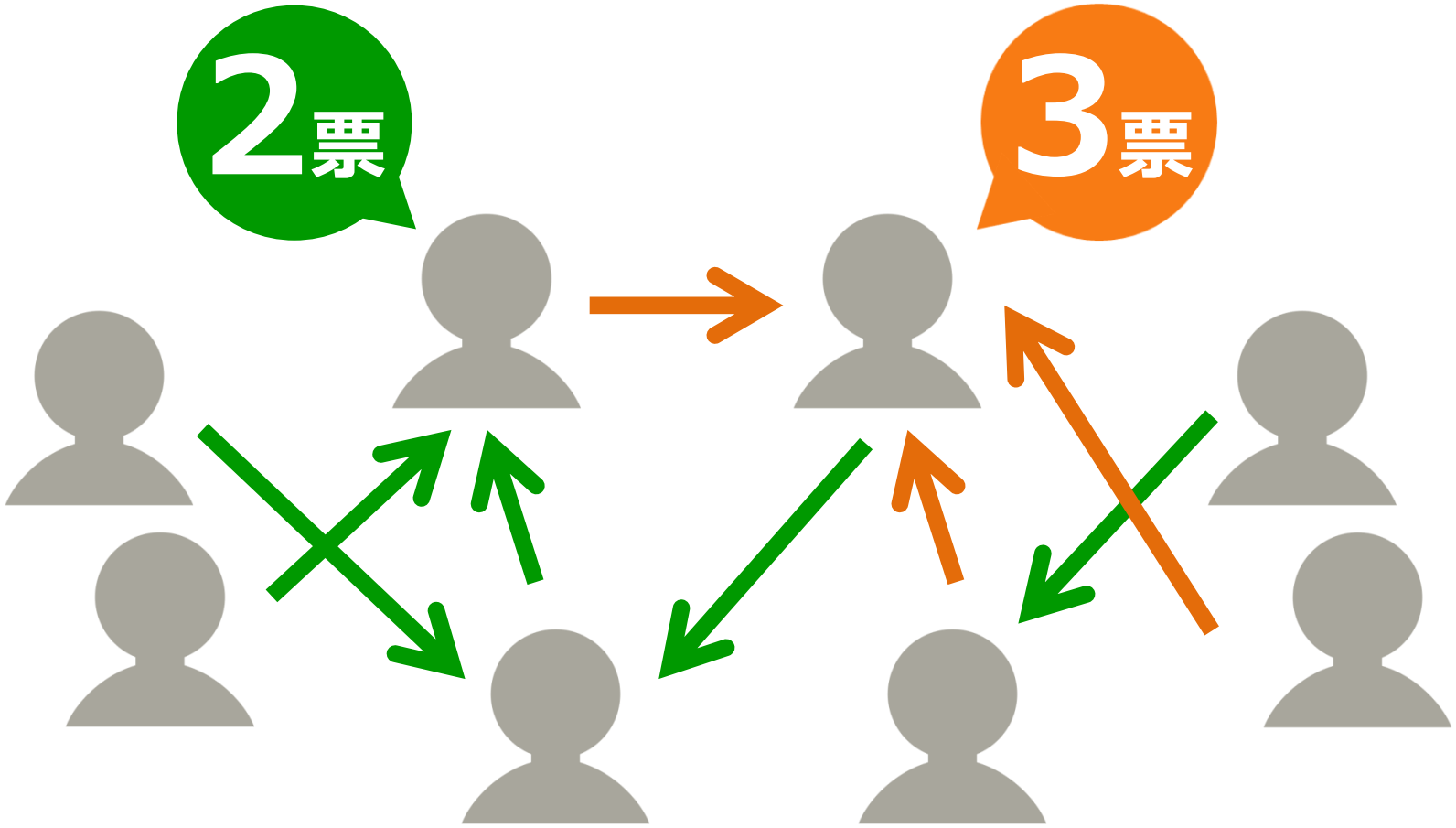
- 最も疑わしい（処遇に不満を抱えている）者を**投票**で決定。



不正調査：解雇処分

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- **<u>最多数の票</u>**を集めたプレイヤーを、**解雇**。



秘密裏の専門調査

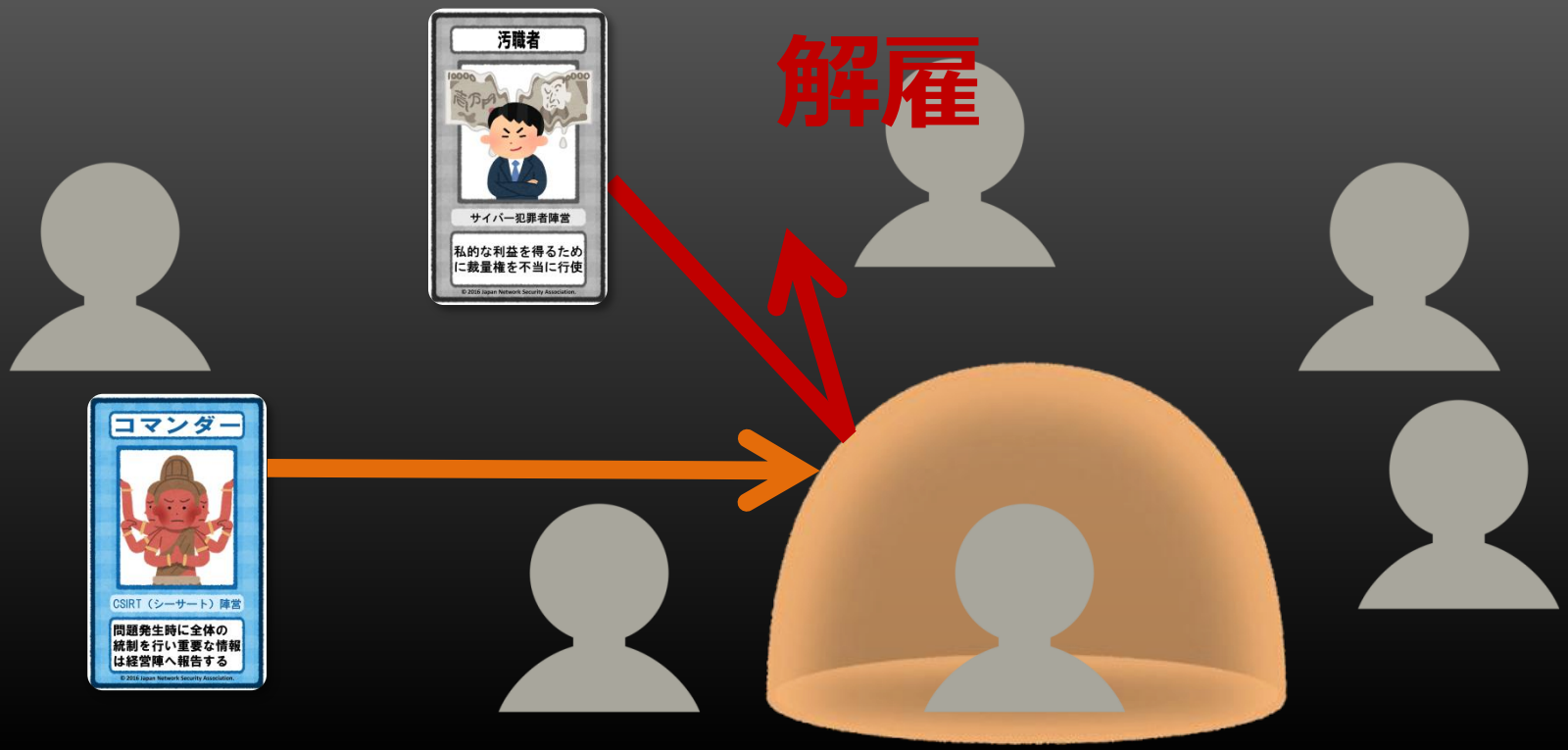
セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- 次の役職には深夜に可能な**専門調査**がある。

専門調査：コマンダー

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- コマンダーは深夜に**護衛調査**を実行する。
- 自分以外の従業員1人に対しそのターンにおける汚職者による**罪の転嫁を防ぐ。**



専門調査：リサーチャー

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- リサーチャーは深夜に**追跡調査**を実行する。
- 先ほど解雇された従業員の**真実（汚職者かそうでないか）を知る**事が可能。

えん罪 解雇

専門調査：フォレンジックエンジニア

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- フォレンジックエンジニアは深夜に**証拠調査**を実行する。
- 任意の一人に対して、いずれの陣営に所属しているのか**真実を知る**事が可能。

解雇

CSIRT

二枚舌なブラックハットハッカー

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- ブラックハットハッカーの勝利条件は
  サイバー犯罪者側陣営の勝利。
- 専門調査による捜査結果は、CSIRT陣営。

解雇

CSIRT

不正実行：汚職者

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- 汚職者は深夜に不正を実行する。
- 罪を着せ、**えん罪に追い込む**プレイヤーを決定する。

解雇

解雇

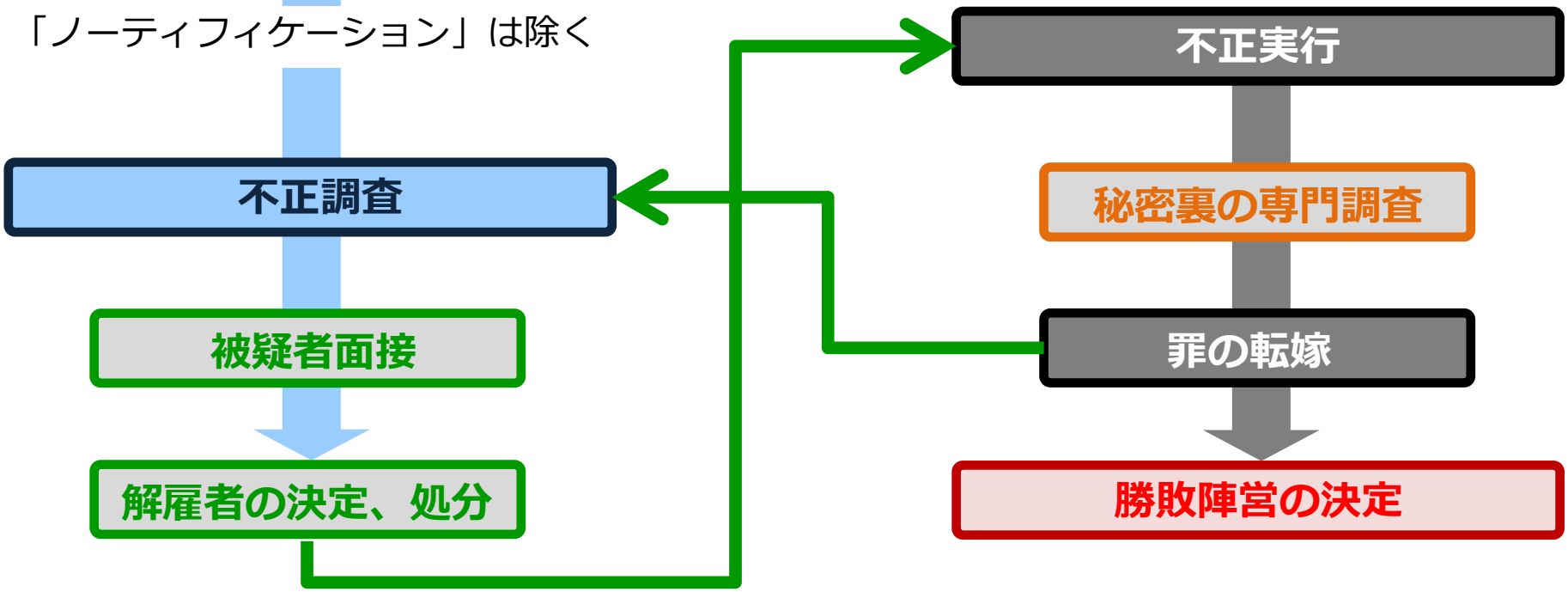
ゲームの進行

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

同役職の相互確認

「ノーティフィケーション」は除く

勝敗陣営が決定するまで、
「不正調査」と**「不正実行」**を**ループ**し続ける。



勝利条件

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

シーサート（CSIRT）陣営の勝利条件

組織内で処遇に不満を抱え不正を繰り返す**汚職者をすべて見つけ出し解雇**できればCSIRT陣営の勝利となります。

サイバー犯罪者陣営の勝利条件

不正を続ける**汚職者と勤続し続けているCSIRTメンバーの人数が同数**となれば、組織は壊滅状態となりサイバー犯罪者陣営の勝利となります。

ゲームスタート

司会者からの指示に従って、アクションを実行していきましょう。

役職配役数、シャッフル

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

- 今回の組合せを発表（11人、1チーム）

×4人

×1人

×1人

×1人

×1人

×2人


記録係×1人

人数が揃わない場合、「汚職者x1」
「フォレンジックエンジニアx1」
「ノーティフィケーションx残り」
「記録係x1」などで対応

ゲームストーリー

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

ホワイトカラーによる不正が後を絶たない…

その夜、内部「**汚職者**」は営業秘密の不正取得を行った。

組織の処遇に不満を抱えていた汚職者は

「**ブラックハットハッカー**」の協力を得て、

犯行に及んだ。

汚職者は自らの自尊心を傷つけた者達へ罪をなすりつけるべく、

毎晩、犯行に及んでゆく。

ひとり、またりひとりと罪なき従業員が解雇されていく…

いったい誰が汚職者なのか？

ゲームストーリー

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

被疑者との面接による不正調査

経営者は一連の事件に対し、不正調査に関する
チーム結成を決断する。**セキュリティ専門家**によって
構成されたチームメンバーはそれぞれの専門性に基づき、
被疑者との面接による不正調査を試みる。

組織の治安を取り戻すべく行われたのは、
毎日一人の解雇者を決定するという過酷な対応であった。
果たして陣営は、すべての汚職者を排除し、
組織の治安を取り戻す事ができるだろうか……。

ゲームストーリー

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

昨夜もまた、内部者による営業秘密の不正取得が発覚しました。
これは、高い特権を持つ汚職者による内部犯行であることは
疑いの余地はありません。

しかし、昼間の汚職者は何食わぬ顔をし、いつもどおり、日々
の業務をこなしている。
しかも、不正調査に関するチームに紛れ込んでいるようです…

汚職者は夜ごとは自らの自尊心を傷つけた者達へ罪をなすりつ
けるべく、毎晩、犯行に及んでいます。
罪を転嫁され、えん罪 解雇された仲間達の為にも、CSIRT陣営
は一刻も早く汚職者を特定し、解雇してください。

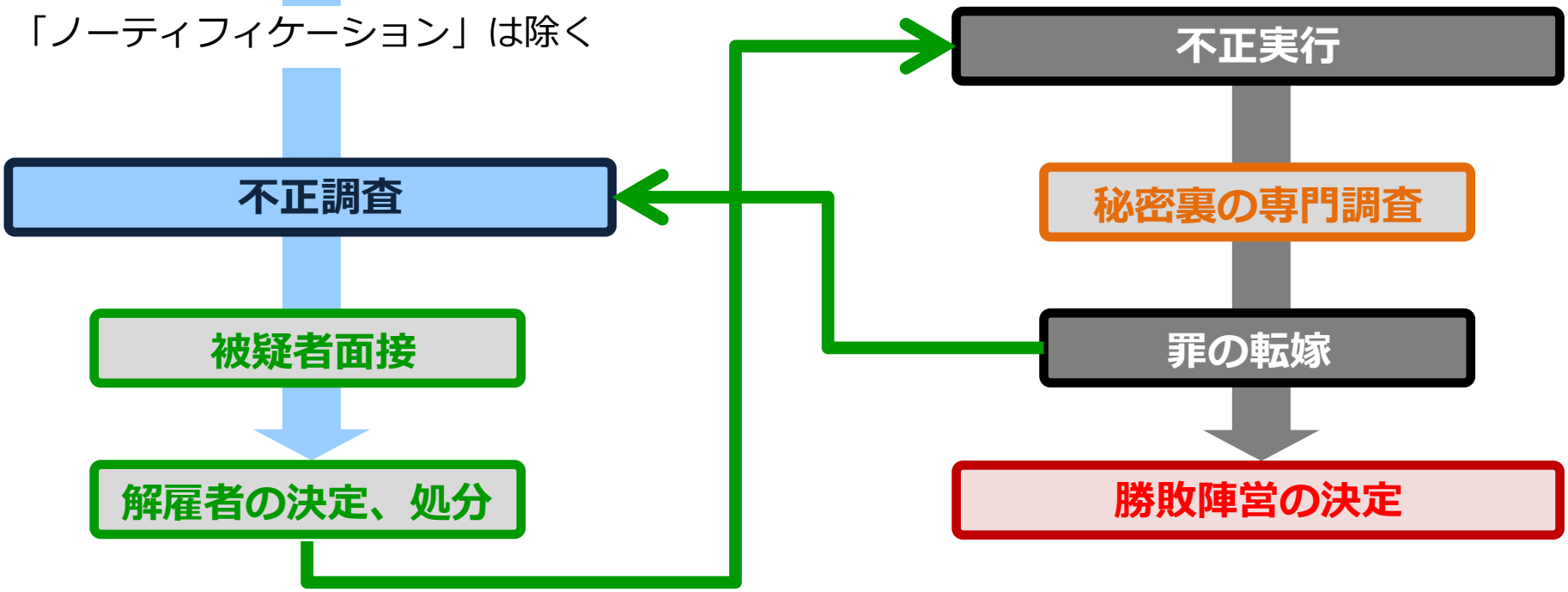
ゲームの進行

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

同役職の相互確認

「ノーティフィケーション」は除く

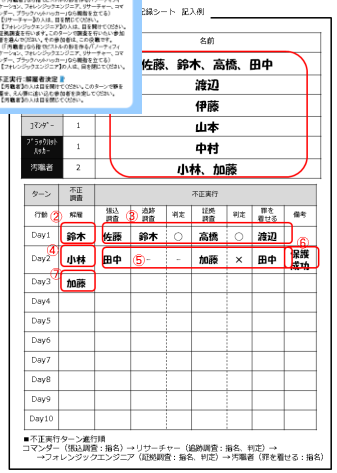
勝敗陣営が決定するまで、
「不正調査」と**「不正実行」**を**ループ**し続ける。



手元に用意してください

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

[役職カード]と[説明書]、[記録シート]を用意



ゲームが終了するまで、
「役職カード」の
内容を
他の参加者へ
明かしてはダメ。

「記録シート」に
記録係は参加者の役職を記入

参加者は役職を予測して
記入していく。

記録係への指示

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

最初の不正実行のときが訪れました。司会者、記録係以外は
みなさん目を閉じ、顔を伏せてください。
記録係の方は、誰がどの役割なのか記録シートに記入していきます。

【汚職者】の方は顔をあげ、目を開け、挙手してください。
汚職者の方、目を閉じ、顔を伏せてください。
【ブラックハットハッカー】の方は顔をあげ、目を開け、挙手してください。
ブラックハットハッカーの方、目を閉じ、顔を伏せてください。
【コマンダー】の方は顔をあげ、目を開け、挙手してください。
コマンダーの方、目を閉じ、顔を伏せてください。
【リサーチャー】の方は顔をあげ、目を開け、挙手してください。
リサーチャーの方、目を閉じ、顔を伏せてください。
【フォレンジックエンジニア】の方は顔をあげ、目を開け、挙手してください。
フォレンジックエンジニアの方、目を閉じ、顔を伏せてください。

不正調査：被疑者面接

記録係の方、すべての参加者の役職は記録できましたか。

それでは、全員顔をあげ、目を開けてください。
このメンバーの中に処遇に不満を抱えた【汚職者】が潜んでいるようです。
これから【5分間】の【被疑者面接（話し合い）】を行います。
「不正のトライアングル」理論や「捜査面接術」を駆使して
手掛かりとなる情報や被疑者の観察を行います。
参加者は真実を話しても、嘘をついてもかまいません。

ただし、役職カードは終了時まで見せてはいけません。

不正調査：解雇者の決定

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

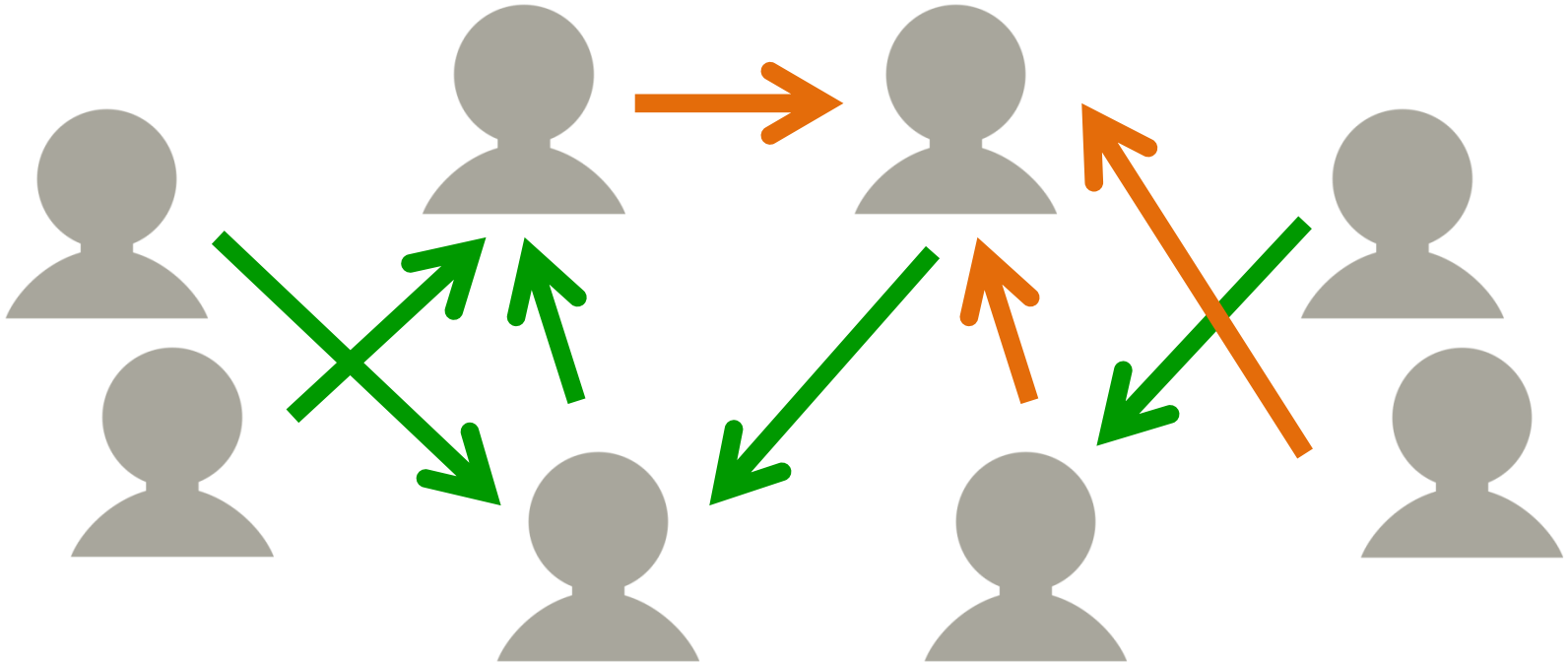
みなさん話し合いを終えてください。これからは発言を一切しないでください。

これより、本日解雇する人の投票を行います。

処遇に不満を抱えている汚職者だと思われる人を指さしてください。

決定した解雇者を【記録シート】に記入してください。

最多投票数が同数の場合には、決選投票を行い1人の解雇者を決定してください。



秘密裏の専門調査

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

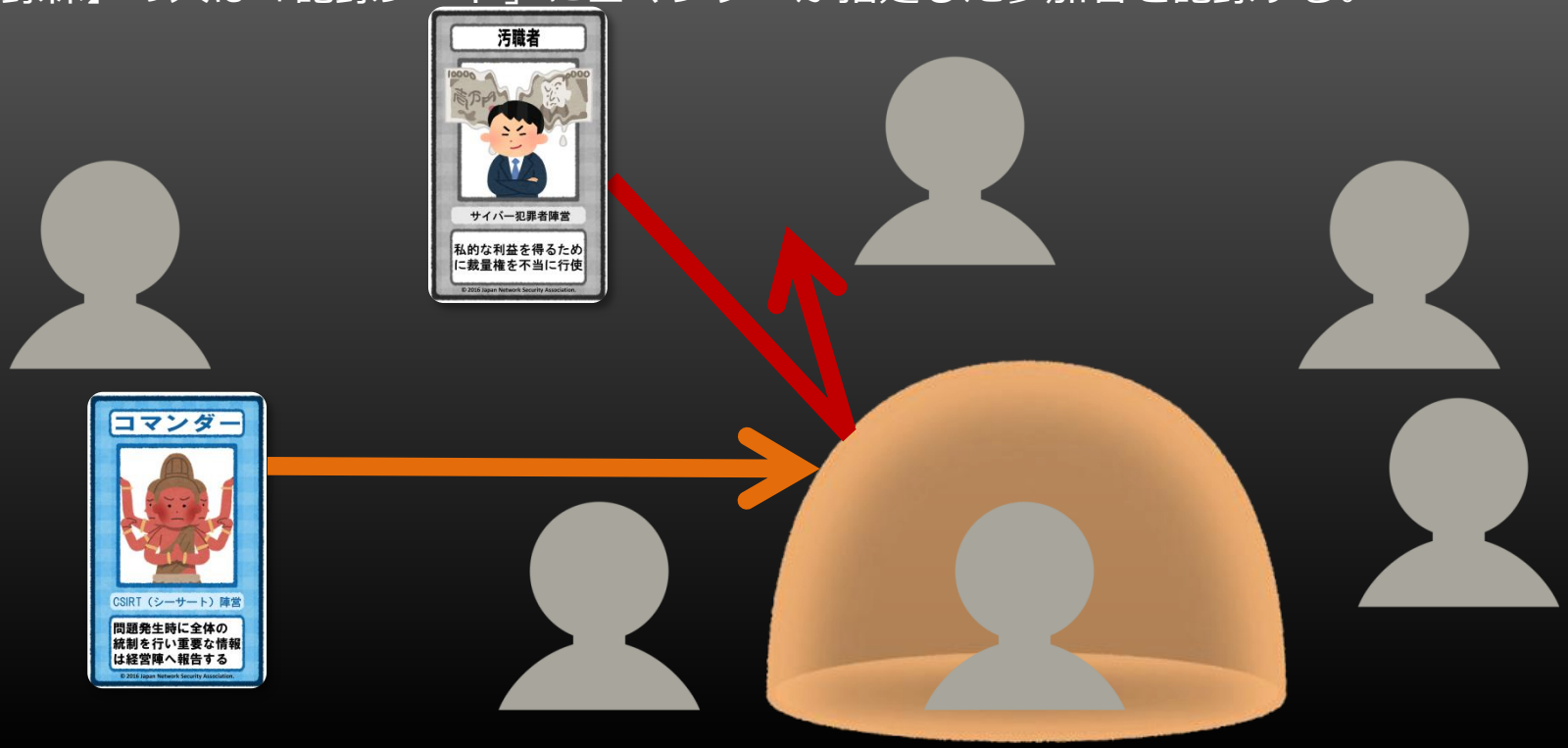
再び闇が訪れました。いまだ【汚職者】はこの中に潜んでいる模様です。
みなさん目を閉じ、顔を伏せてください。
記録係の方は、これから【専門調査】における結果を司会者が指示する
ジェスチャーで参加者に示してください。

【リサーチャー】の人は、目を開けてください。【追跡調査】を行います。先ほどの不正調査で追放された参加者はこの役職でした。
（「汚職者」なら指でピストルの形を作る/「CSIRT陣営」または「ブラックハットハッカー」）なら親指を立てる）
【リサーチャー】の人は、目を閉じてください。
【フォレンジックエンジニア】の人は、目を開けてください。【証拠調査】を行います。
このターンで証拠調査したい参加者を選んでください。その参加者はこの役職です。
（「汚職者」なら指でピストルの形を作る/「CSIRT陣営」または「ブラックハットハッカー」）なら親指を立てる）
【フォレンジックエンジニア】の人は目を閉じてください。

専門調査：コマンダー

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

【コマンダー】の人は、目を開けてください。護衛調査を行います。
このターンで罪のなすり付けを防ぎ、守りたい参加者を選んでください。
ただし、前のターンと同じ参加者、自分自身は選択することができません。
【コマンダー】の人は、目を閉じてください。
※【記録係】の人は「記録シート」にコマンダーが指定した参加者を記録する。



不正実行：汚職者

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

【汚職者】の人は、目を開けてください。不正を働くときが訪れました。
自らの自尊心を傷つけたと思う者は誰ですか。罪を着せ、えん罪に追い込む参加者を決定してください。
【汚職者】の人は、目を閉じてください。
※【記録係】の人は「記録シート」に汚職者が指定した参加者を記録する。

解雇

記録係への指示

それでは、全員顔をあげ、目を開けてください。

先ほど不正実行のターンで汚職者に罪を転嫁され解雇された人を
記録係の方は参加者へ報告してください。
「○○さんでした」　or　「いませんでした」（コマンダーによる保護が成功）
解雇された人はテーブルから離れて組織の行方を見守ってください。
参加者の発言を「機会」、「動機」、「正当化」の観点から
自分なり分析してみてください。

記録係の方は残りの比率を参加者へ報告してください。
「CSIRT陣営は○人、サイバー犯罪者陣営は○人です。」
※勝利条件を確認（※スライド18）

ゲームは続きます（※スライド27へ戻る。）…

捜査面接術

Investigative Interview

無実の人々と犯罪者を見極める

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

「汚職者」は自白しない！

相手に事実を
述べさせるよう
仕向ける。

※動かない事実を探る
※面接者は常に事実を述べて罪を問う

NGワード：

「あなたがやったのですか」
※感情的にさせる言葉の使用は避ける
※一度、被疑者が不正行為を否定した場合、その状況の克服は困難

被疑者の表情や仕草を観察

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

無実の人が示す特徴を知る

- 罪に問われるとショックを受ける
- 怒りを露わにする
- 強く否定する

被疑者の表情や仕草を観察

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

犯罪者は黙り込む

- きつく口を結ぶ
  - ストレスや不安を感じてる状態
  - 口を触るなども同様の傾向
- 声が高くなる、トーン変化
  - 高音は冷静さを失っている傾向
- 否定が弱々しい
  - 同じ言葉を反復する（時間稼ぎする）
  - 発言が短くなる、曖昧になる
  - 真っ向否定ではなく説明傾向が強くなる
  - 協力的な行動が減る

役職別攻略法

CSIRT（シーサート）陣営編

誠実に…、積極的に…

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

ノーティフィケーションによる騙りは御法度

- 情報が何も得られないとき（平時）には、自ら率先して情報収集に取り組む
- ステークホルダーを探し共闘を持ちかける
- 怪しい振る舞いを推理していく

コマンダーに共闘を願う

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

証拠調査能力をアピールし、保護を求める

- 活躍すべきタイミングは2ターン目から
- 「捜査面接術」だけでは確証が持てない人物を探る
- 「汚職者」による騙りには論理的に自分の証拠能力が正当であることを証明する

証拠の信憑性を検証

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

フォレンジックエンジニアの能力を検証

- まずは隠密行動で異常値（汚職者）の発見に徹する
- 疑わしきフォレンジックエンジニアが登場したときには証拠調査能力の検証役に徹する

保護すべき対象を決定

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

全体像を考慮し、「**トリアージ**」を行う

- 保護すべき対象を重要度に応じて選別（triage）する能力が必要
- フォレンジックエンジニアの保護が重要度「高」
- 他のCSIRTメンバーに護衛先を決めてもらう調整役を引き受ける戦略も有効

役職別攻略法

サイバー犯罪者陣営編

技能による暗躍を試みる

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

専門調査能力を持っていると思い込ませる

- 「フォレンジックエンジニア」や「リサーチャー」のように振る舞う
- 「コマンダー」による護衛を受ける
- 調査結果がCSIRT陣営となることを有効活用する

CSIRT陣営を欺く

セキュリティ専門家人狼（JIN-ROH）
SECWERE WOLF

自分に不利な専門能力を持つ者に罪を着せる

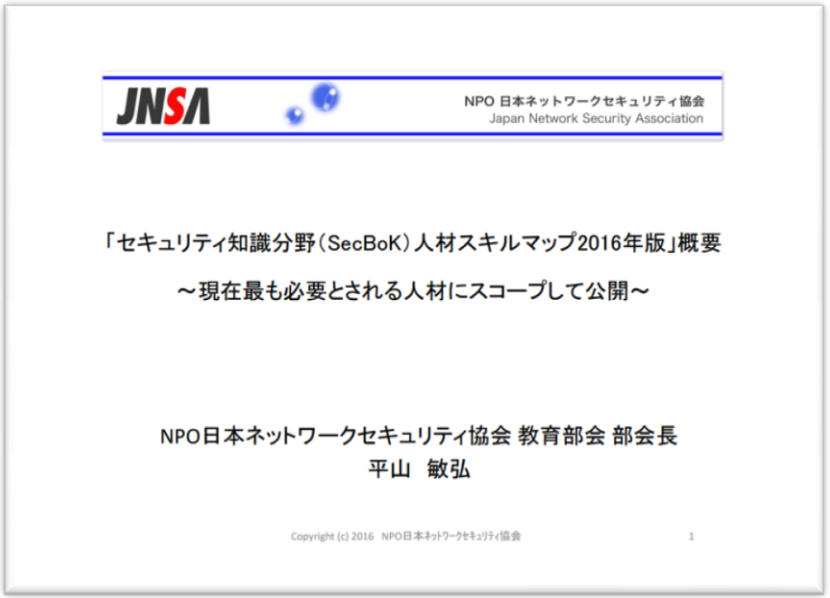
- 役職を騙り、CSIRT陣営を混乱へと導く
- 戦略的な身内との裏切りも有効
- 同士討ちさせ、サイバー犯罪者陣営の勝利を目指す

参考資料

さらなる学習に向けて…

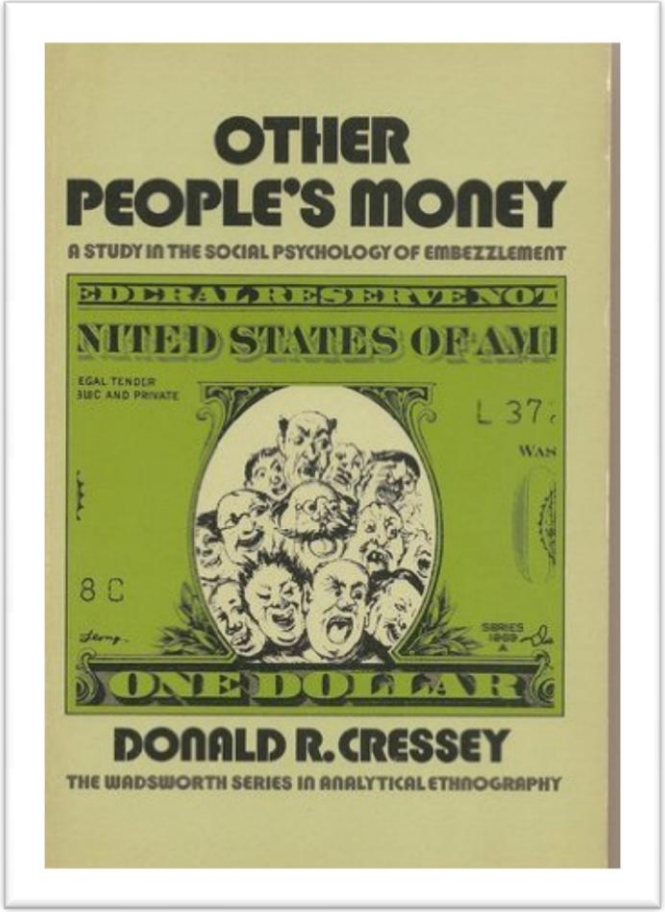
CSIRT
人材のスキル＆コンピテンシー

日本コンピュータセキュリティインシデント対応チーム協議会
『CSIRT人材の定義と確保(Ver.1.0)』



特定非営利活動法人 日本ネットワークセキュリティ協会
『セキュリティ知識分野（SecBoK）人材スキルマップ2016年版』

不正のトライアングル

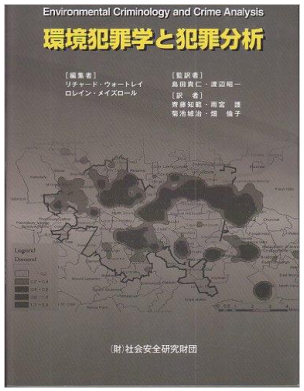


クレッシー・ドナルド・R 1953年『他人の金（Other People's Money）』 フリープレス社、ニューヨーク（New York: Free Press）

特定非営利活動法人 日本ネットワークセキュリティ協会
『内部不正対策 14 の論点』

情報システムへの
状況的犯罪予防論の適用

セキュリティ専門家人狼（JIN-ROH）
SECURE WOLF



(財)社会安全研究財団 2010年
『環境犯罪学と犯罪分析』

状況的犯罪予防における25の技法

Twenty Five Techniques of Situation Prevention

Increase the Effect 犯行を難しくする	Increase the Risk 捕まるリスクを高める	Reduce the Rewards 犯行の見返りを減らす	Reduce Provocations 犯行の挑発を減らす	Remove Excuses 釈明させない
対象を防御的に強化する	監視者を増やす	標的を隠す（存在がわからない）	欲求不満やストレスを減らす	規則を決める
施設への出入りを制限する	自然監視を補佐する	対象を排除する（存在をなくす）	対立（紛争）を避ける	指示を提示する
出口の検査	匿名性を減らす	所有者の特定	誘惑や興奮の低減	良心に警告する
犯罪者をそらす	現場管理者の利用	市場を阻止	仲間からの圧力を緩和する	遵守を補佐する
道具や武器を制御する	フォーマルな監視体制を強化する	便益を与えない	模倣犯を阻止する	薬物・アルコールを規制する

対策の指針＆具体的な実施策

独立行政法人情報処理推進機構
『組織における内部不正防止ガイドライン 第3版（2015年3月改訂）』

特定非営利活動法人 日本ネットワークセキュリティ協会
『内部不正対策ソリューションガイド』