

サイバーセキュリティ演習:

# Kaspersky Interactive Protection Simulation (KIPS)

2024年12月13日  
株式会社カスペルスキー  
セールスエンジニアリング本部

V1.1

# Kaspersky Interactive Protection Simulation (KIPS)とは



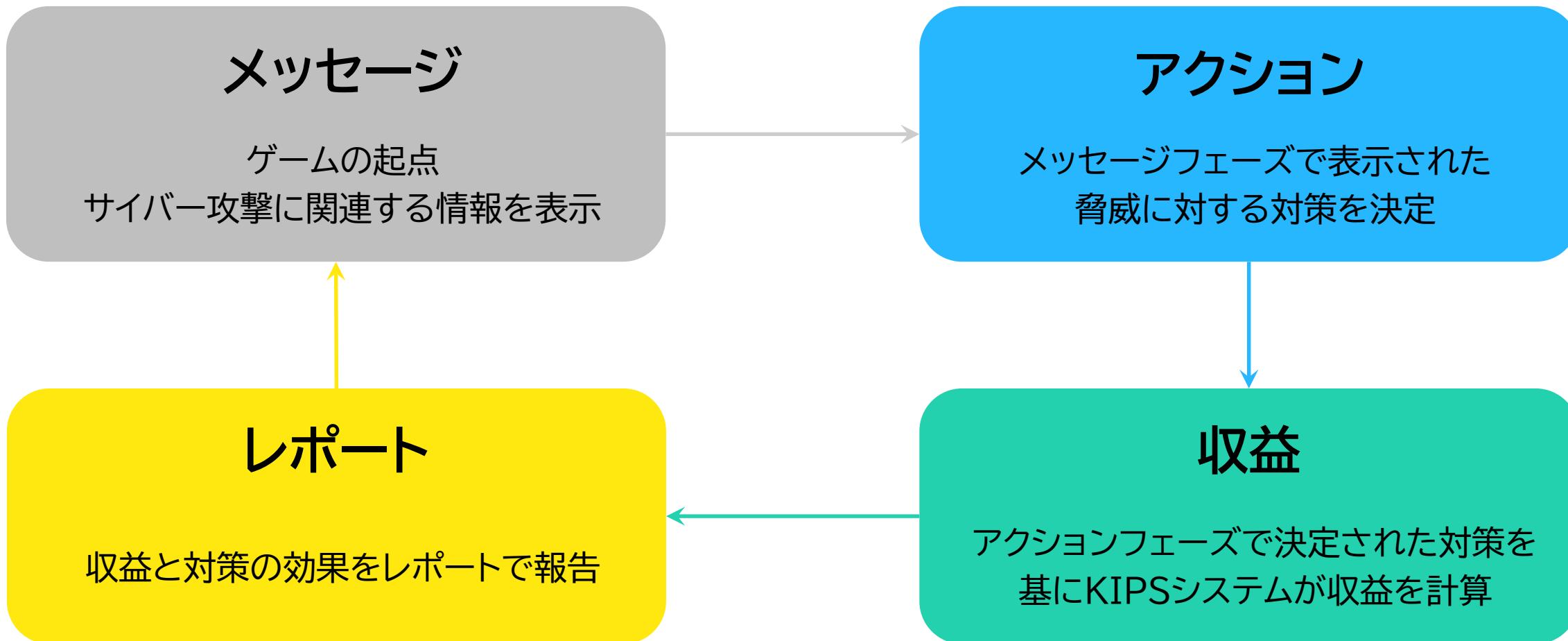
## ■ゲーミフィケーション理論に基づいて開発されたゲーム形式の対サイバー演習

- ・ゲーム形式でセキュリティインシデントを体験することで、サイバー攻撃が企業に与える影響を理解し、限られたリソースで被害を最小化するためのインシデント対応策を学習
- ・受講者の選択が次のステップに影響するインタラクティブ構成、同じシナリオでも複数回体験することで、サイバーセキュリティ対策を深く理解することが可能
- ・共同作業でチームワークを育成し、チーム間の競争を通じて分析スキルを向上  
ゲーム終了後に参加者全体でディスカッションをすることで改善点・ポイントを共有
- ・ランサムウェアや標的型攻撃など、すべての企業を対象としたシナリオに加えて、産業用システムの稼働環境・業界固有のサイバー攻撃など特定業種に特化したシナリオも用意

# ゲームの流れ



■参加者は1ターン:4つのフェーズで構成される全5ターンのゲームに参加





# ゲームの流れ:メッセージフェーズ

- ・メッセージボードに表示されたインシデントやサイバー攻撃に関連するニュースを確認し、企業を保護するために必要な対策をチームで協議

The screenshot shows a game interface with a message board. A red box highlights the top status bar containing the timer (09:58), current turn (ターン01), sales figures (\$0), and team name (#1 Demo). Another red box highlights the message board content, which includes a news article about a shellshock vulnerability. A third red box highlights the bottom status bar showing budget (\$250 K) and time (100). Red arrows point from Japanese labels to these elements.

残り時間

現在のターン

予算・時間

チーム名

収益

メッセージボード  
インシデントや  
サイバー攻撃に  
関連するニュースを  
表示



# ゲームの流れ:アクションフェーズ

- インシデントに対して最適な対策をアクションカードから選択
- 各カードに「コスト」と「時間」が設定、「時間」は各ターン100秒、「予算」は全てのターンで\$250,000に収まるように選択
- 1回限り使用可能な「SW/HW」・「ワンタイムサービス」と何度でも使用可能な「リニューサブル」の3種類

SW/HW	ワンタイムサービス	リニューサブル
<p>1</p> <p>オフィスネットワークにバックアップ&amp;復旧サーバーを導入</p> <p>バックアップ&amp;復旧サーバーを購入して設置します。サーバーはオフィスワークステーションのフルバックアップ(ディスクイメージ)を各ターンの終わりに実施します。</p> <p>\$40 000 35</p> <p>カードをクリックして選択</p>	<p>7</p> <p>セキュリティ監査の実施</p> <p>セキュリティコンサルタントを雇ってセキュリティシステムとポリシーのアセスメントを実施します。セキュリティを向上するためのヒントを得ましょう。</p> <p>\$10 000 40</p> <p>カードをクリックして選択</p>	<p>8</p> <p>ペネトレーションテストの実施</p> <p>セキュリティ専門家を雇って企業のペネトレーションテストを実施します。これは、脆弱性とセキュリティ上の課題を明らかにし、解決するための提案を得ることができます。セキュリティホールが見つければ業務に支障があるでしょう。</p> <p>\$10 000 10</p> <p>カードをクリックして選択</p>

左:予算 右:時間

対策の詳細



## ゲームの流れ:収益フェーズ

- 選択したアクションカードを基にKIPSシステムが収益を計算
  - >各ターン最大\$200,000、5ターンで\$1,000,000の収益を獲得
- さらに、長期的なセキュリティ対策を実施できた場合、ボーナス最大\$100,000を獲得
- 各チームは「事業継続」と「\$1,100,000の収益獲得」を目指して、セキュリティインシデントを対処

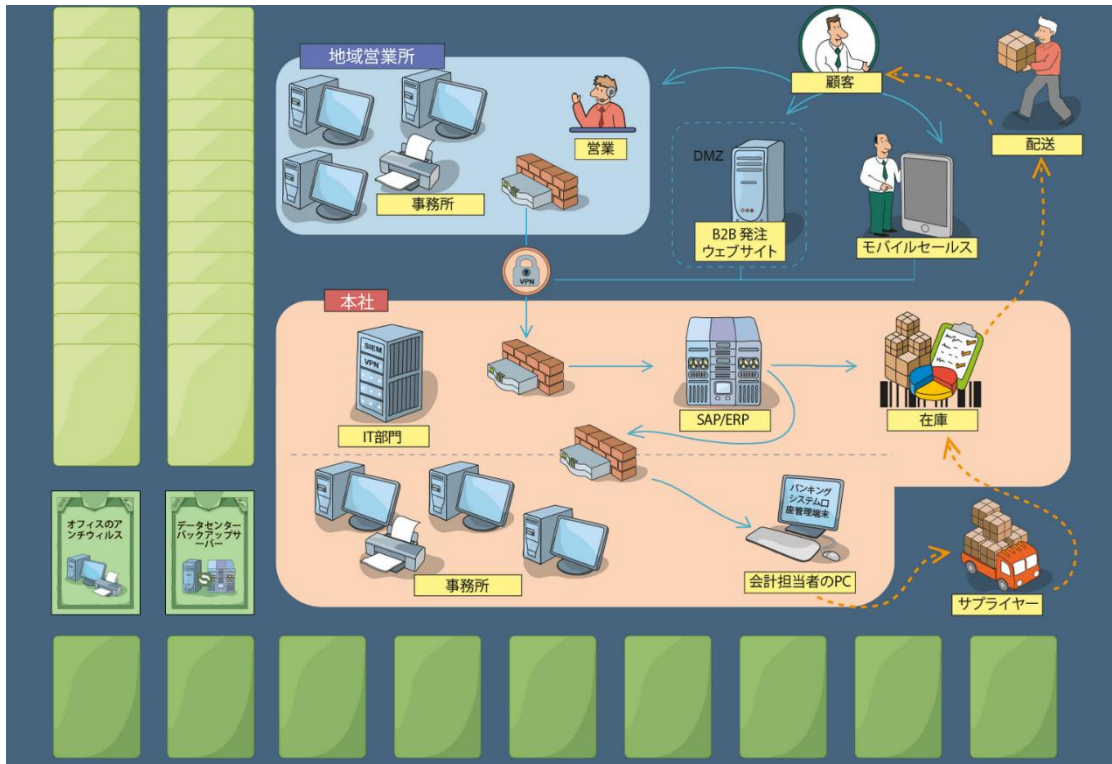


# 業界に特化した複数のシナリオ



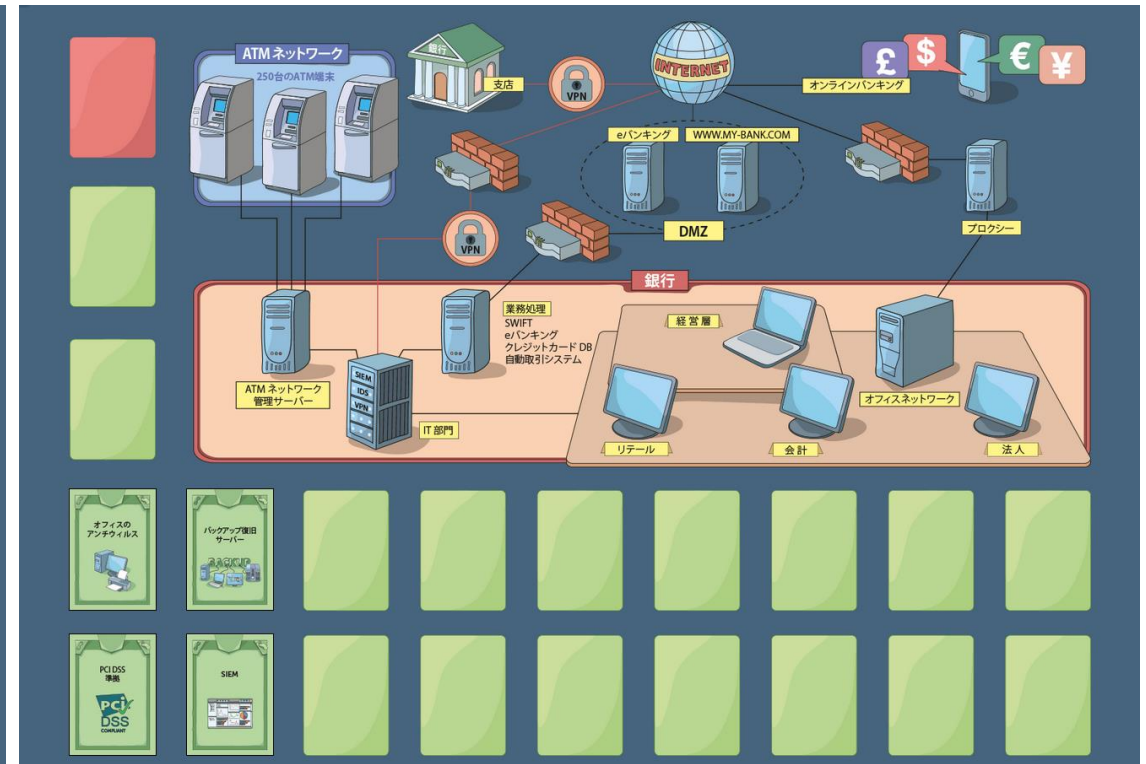
## シナリオ1: 企業

- ・直営・オンライン経由で商品を販売する企業をAPT、Shellshock、ランサムウェア、インサイダー脅威から保護



## シナリオ2: 銀行

- ・貿易業務、オンラインバンクを運営する銀行をCarbanak、Tyupkin、Cryptor、Black Energyから保護



# 業界に特化した複数のシナリオ

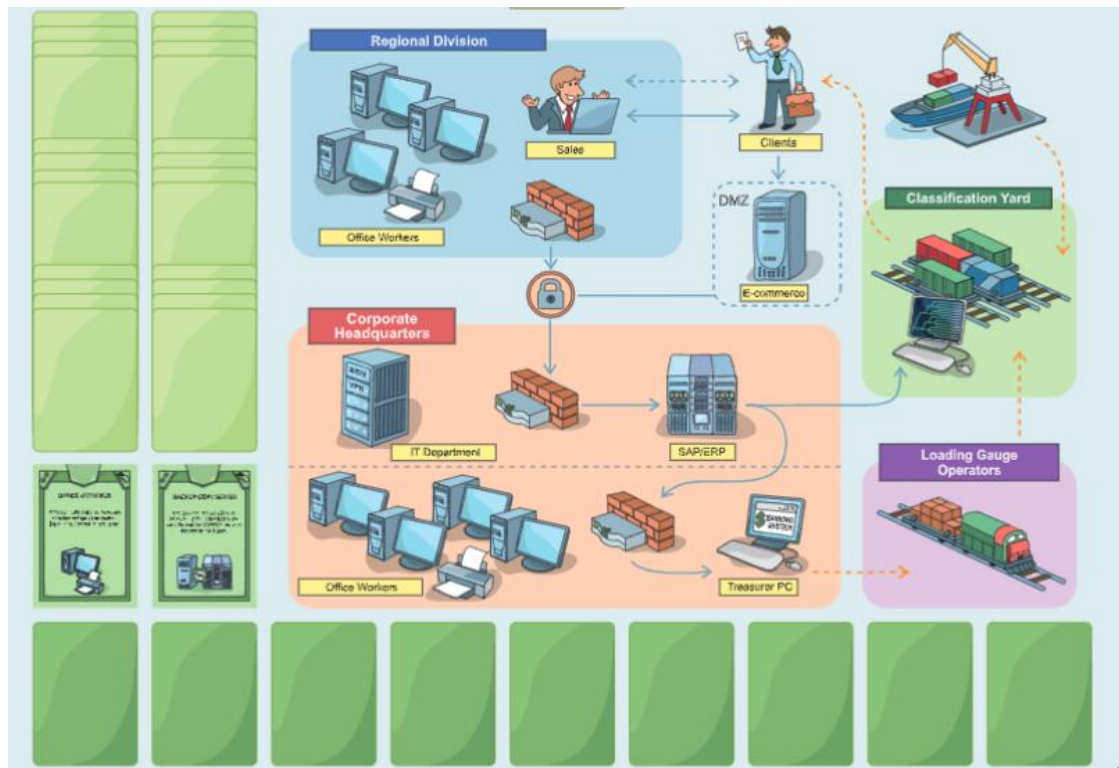
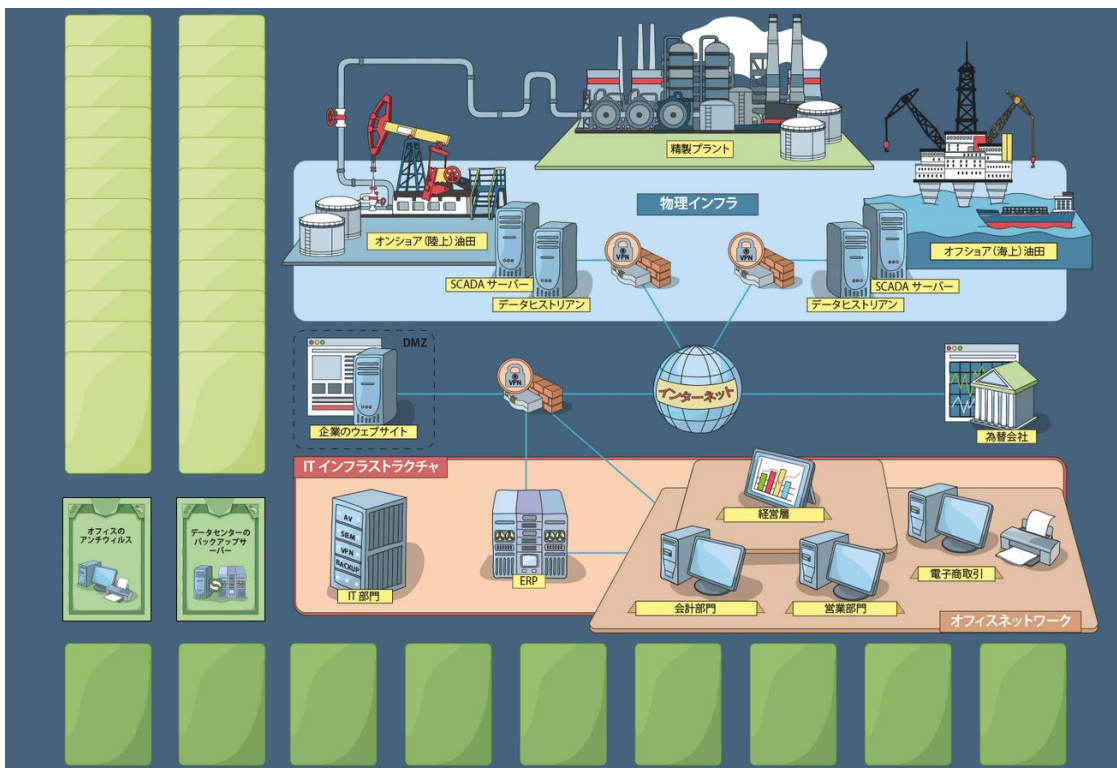


## シナリオ3: 石油ガス

- ・SCADAシステムによって制御された油田を狙う  
ランサムウェア・マルウェア・APTから保護

## シナリオ4: 運輸

- ・運営する物流会社を襲うHeartbleed、ランサムウェア、  
APT、インサイダー脅威に対処



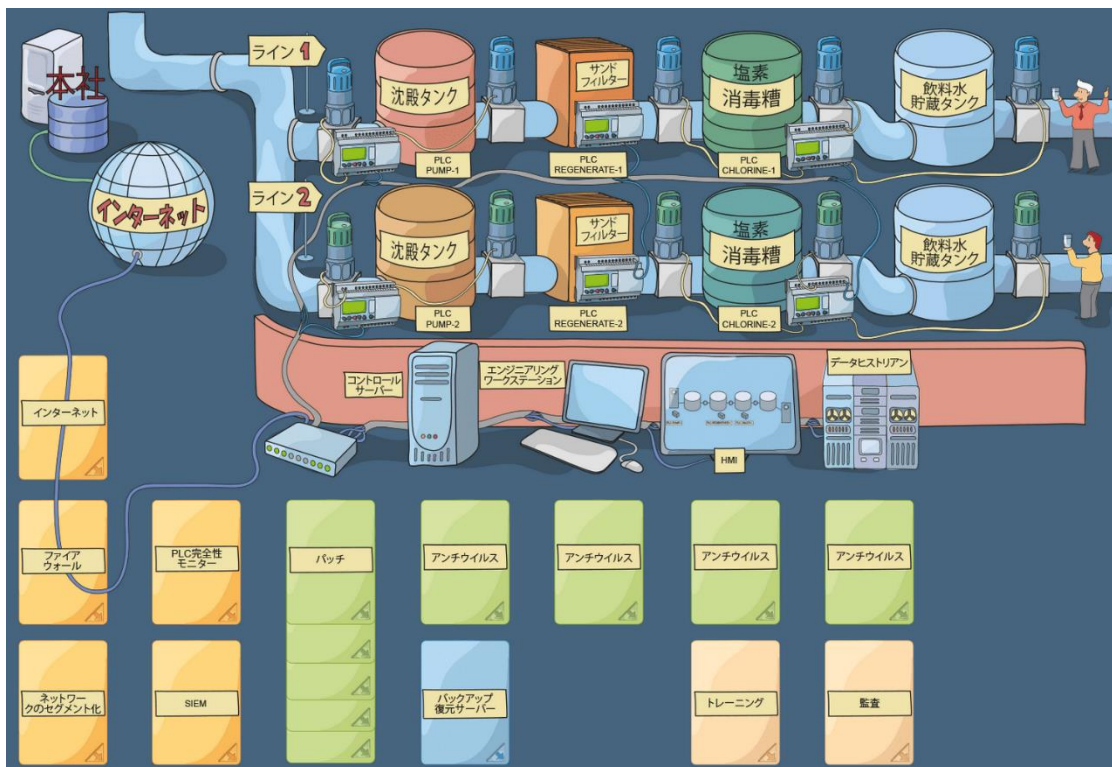


# 業界に特化した複数のシナリオ



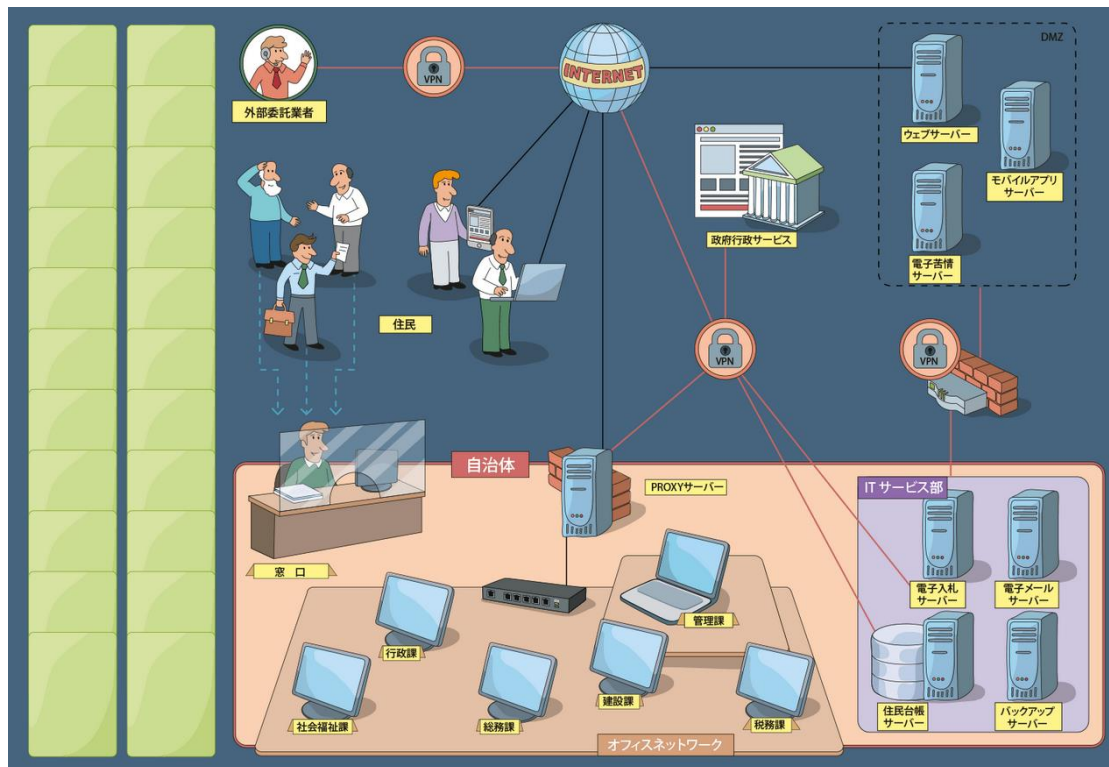
## シナリオ5: 発電所・浄水場

- ・発電所・浄水場を襲うStuxnetからITインフラと2つの生産ラインの安全性を確保



## シナリオ6: 地方行政

- ・市民から高い評価を得られるように脅威からインフラ・サービスを保護し、機密情報の流出を阻止



# ゲーム形式



ライブ・オンライン、2つの形態でゲームを実施可能

## ライブ (会場実施)

全参加者が同じ会場でゲームに参加

### <特徴>

- ・最大受講者数:80人 (20チームまで)
- ・3~4人/1チーム
- ・全参加者が同一言語
- ・トレーナー・アシスタントが出席
- ・主に印刷された教材を使用



## オンライン

PC・タブレットからゲームに参加  
(ライブと組み合わせ可能)

### <特徴>

- ・最大受講者数:1000人 (300チームまで)
- ・チームごとに異なる言語が選択可能
- ・トレーナーはWeb会議ツールを使用してゲームを先導



**kaspersky**