

# Comparing Insider IT Sabotage and Espionage : A Model-Based Analysis

総合政策学部4年 矢部竜太

## 資料概要

---

- } 内部の人間によるサボタージュとエスピオナージュはどのような状況で起こるのかを調べ、予防に役立てることが目的
  
- } 本発表で取り扱う内容
  1. Stressful Event ,Organizational Sanctions
  2. Concerning Behavior
  3. Technical actions
  4. Rule Violations
  5. Lack of physical and electronic access control



# Stressful Event

---

## } Stressful Eventとは

} 職場などで起きるいやな出来事 (同僚との衝突や解雇)

1. 個人のニーズが増大
2. 技術的危険や違反行為が増大
3. 違反行為により制裁が下される
4. 制裁によるインサイダーのストレスが増える

} この時、個人のニーズは個人的な性質の影響により加速する

} また、Stressful Eventによりインサイダーのストレスが増える

} Stressful Eventはその人間がもともと持っていた性質によって引き起こされる場合もある

} 内部犯行の92%はStressful Eventの影響があった

---



# Stressful Event事例 (IT サボタージュ )

---

## } サボタージュを起こした人間の特徴

### } 個人的な性質

- } セキュリティチェック選抜用紙をごまかした
- } ドラッグ歴あり
- } 不倫で前職をクビになった
- } ドラッグ使用の過去の話を使い詰められても認めない

### } 仕事上の個人の性質

- } 人種差別・セクハラ発言
- } 仕事に遅刻する、また直ぐに帰る
- } 職場から姿を度々消す
- } システムの不備や顧客の要求を無視



## Stressful Event事例 (IT サボタージュ )

---

- } で述べたような振る舞いを行う人間に対する職場の人間の不信
- } 衝突が発生
- } 職場のサーバへの不正アクセス等を行うように
- } そのことが発覚しクビになりかける
- } 社内サーバにロジックボムを仕掛け、解雇通知をサーバ内のデータ群ごと破壊



## Stressful Event事例(エスピオナージ)

---

### } Brian Patrick Reganによるエスピオナージ事例

- } 過去にイラクと中国のミサイルに関する文書をデータベースへの不正アクセスにより入手し、持ち出したことがある
  - } 職場の同僚等、身近な人間に対する不平、不満を漏らす
  - } アスリートへの寄付等に熱中していたため、多額の借金をかかえ財政的にも苦しかった
  - } 子供が4人おり、大学の学費の支払いの問題などもあった
- 
- } 中国、イラク、リビアへ重要文書の売却を行う



# Concerning Behavior

---

## } Concerning Behaviorとは？

- } 内部犯行を試みようとする人間に見られる兆候
  - } 遅刻、ずる休み
  - } 同僚との論争
  - } 仕事のパフォーマンス低下
  - } 職場における規約違反
  - } 犯行準備
- } 実際にあった事例のうち97%は、上司や同僚がこれらの兆候を把握していた
- } 兆候は実際に犯行に及ぶ1～48か月前に見られる
- } その徴候がみられる期間はおよそ12日～19か月



## Concerning Behavior事例(IT サボタージュ)

---

- } クビにされた後、会社のサーバへのリモートアクセスを試みたITエンジニア
  - } 二種類の社会保障番号を持っていた
  - } コンピュータルームにWebカメラを設置
  - } 同僚に暴言、またそれ以外にも「俺が王だ」や「俺が大統領だ」等の大言壮語
  - } 仕事中のミスや内職が目立つようになった



## Concerning Behavior事例(エスピオナーズ)

---

- } 国家機密を売ったCIA職員
  - } アルコール依存
  - } アルコール依存による対人関係の不和
  - } 借金等の財政上のストレス
  - } ニューヨーク地下鉄で重要書類紛失
    - } 口頭懲戒のみ
  - } 上司の検査・カウンセリング要請を、血液検査は受け入れたがカウンセリングは拒否



# Technical action

---

- } Technical Indicatorとは？
  - } 内部犯行のリスク増加を示す事象の発生や状況等
- } エスピオナージとIT サボタージュでとる行動が異なる
  - } IT サボタージュの場合
    - } バックドアをサーバに仕込むなど様々な準備が必要
    - } 様々な方法が用いられるが、使用は一回きり
    - } 結果として情報流出も起こる (それが目的ではない)
  - } エスピオナージの場合
    - } 情報をコピーして持ち出したりするだけなので気付かれにくい
- } 問題点
  - } Trust Trapにより内部犯行への組織の抵抗力が落ちやすい



# Technical action(Trust Trap)

---

## } Trust Trapとは？

1. 内部の人間が信頼を得る
2. 検査・監視が緩くなる
3. その結果不正が探知されづらくなる
4. 不正が探知されないため、内部の人間をますます信頼する
5. その結果検査・監視が緩くなる

} 1～5の繰り返し



## Technical Indicator事例(IT サボタージュ)

---

- } 組織のサーバにロジックボムをしかけたITエンジニア
    - } 社内で降格 + 同僚との衝突
    - } 何年もかけて社内にオリジナルのネットワークを構築
    - } 行動が不審と上司に首にされかけるが、問題が今までなかったため、会社のオーナーがその判定を覆す
    - } その後、人事権を巡って社内でまた争いクビに
    - } システムのバックアップデータを持ち逃げ
    - } ロジックボムを作成し、自身が構築したネットワーク経由でサーバに仕掛ける
    - } ロジックボムをしかけたサーバに社内の情報やプログラムが入ったファイルを集めた後、まとめて破壊
    - } 被害額は約1000万ドル
- 



# Technical Indicator事例(エスピオナーズ)

---

## } Robert Hanssen

- } FBIのエージェント
- } ソビエトとつながりがあった
- } 自身の権限でアクセスできる以上の情報にアクセスし、ロシアに流出させていた
- } 1979年にソビエト崩壊の結果、内部工作を行う心配はもうないと判断し、監視・検査を緩めた
- } FBIの事件記録へNeed To Know以上の情報へのアクセスを行った
- } そのアクセスログは残っていたが、ログのレビューを行わなかった



# Rule Violations

---

## } Rule Violations

### } 組織内における違反行為

} パスワードチェッカーのダウンロード等が挙げられる

### } Concealing Rule due to organization sanctions(B4)

1. 組織の制裁は内通者の行動への制裁を強化
2. 制裁強化はインサイダーに危険を察知させる
3. 危険を察知したインサイダーはルール違反痕跡を隠す
4. ルール違反隠しは組織の制裁を抑止

### } Reducing violations due to organization sanction (B3)

1. インサイダーの有害行動
2. 有害行動が違反行動の特定を強化
3. その結果、制裁が強化される

### } Unobserved emboldening of insider (R3)

1. 違反行為や技術的な危険の増大が組織の制裁を強化
  2. 制裁を恐れるインサイダーが危険を察知
  3. インサイダーが危険を恐れる結果違反行為等を自粛
- 



## Rule Violations事例(IT サボタージュ)

---

- } とある企業で作成中のプログラムに意図的にバックドアを仕込んだITエンジニア
  - } ソースコードを意図的にややこしく書き、製品に仕込んだバックドアの存在を隠ぺいしていた
- } 製品が完成した際、自身がソースコードのバックアップデータの管理を社内の方針に背いて行っていたことを申告し退職した
- } 内部犯行者退職後、製品の不備を企業自身が修復することができないが、内部犯行者はその製品への不正アクセスを繰り返した



## Rule Violations事例(エスピオナージ)

---

- } Technical Indicator事例におけるRobert Hanssen
  - } パスワードチェッカーやクラッキングプログラムのインストール
  - } 発覚後はカラープリンタのドライバをインストールしようとしたとの言い逃れ 処罰なし
  - } 監視・検査の改善がなされない状況で行為がエスカレートしていった (FBIのセキュリティシステムの不備を発見しロシアに報告する等の行い)



# Lack of physical and electronic access control

---

- } Lack of physical and electronic access controlとは？
  - } 物理的、電子的なアクセスコントロールの不備が違反行為を生み出す
- } Restricting authorized access level(B2)
  1. インサイダーが内部システムにアクセス
  2. 不正アクセス探知が強化
  3. 組織が危険を探知
  4. 組織の危険探知によるインサイダー内部アクセスの抑止
- } Organization response to unauthorized access(R3)
  1. 不正アクセスの探知
  2. 組織が危険を探知
  3. 監査とモニタリングの強化
- } Trust trap(R2)
  1. 監査とモニタリングの強化
  2. 危害活動の発見
  3. 組織が危険を探知
- } Harmful action control by enforcing access controls (B5)
  1. 危害活動が行われる
  2. 組織が危害活動を探知
  3. 組織が危険を察知する
  4. アクセスコントロールを強化
  5. インサイダーの違反行為等を抑止
- } **アクセスコントロールとターゲットを絞った監視・検査を組み合わせることが必要**



## Lack of physical and electronic access control事例 IT サボタージュ

---

- } 緊急時の電話への情報配信サービスを行う会社
  - } 内部工作の兆しを察知し、NOC (ネットワークオペレーションセンター) への物理的なアクセス制限
  - } NOCのネットワークへアクセスできる端末への物理的なアクセス制限
  - } システムの管理は不十分だった
- 
- } 内部犯行者は管理者のアクセスカードを手に入れたのち、NOCへのアクセスを行った
- 



## Lack of physical and electronic access control事例

### エスピオナーズ

---

- } Leandro Argocillo
  - } ホワイトハウスのセキュリティ管理役員
  - } フィリピン人であり、フィリピン大統領と親密だった
  - } フィリピン大統領と個人的に会う間柄にも関わらず、監視・検査の強化を行わなかった
  - } Leandroは自身の権限で手に入る範囲の情報をフィリピンに流出させていた
- 

