STAMPを用いた包括的なリスクマネジメント手法の研究

千葉工業大学　社会システム科学部　金融・経営リスク科学科
板橋 聖馬

目次

研究背景

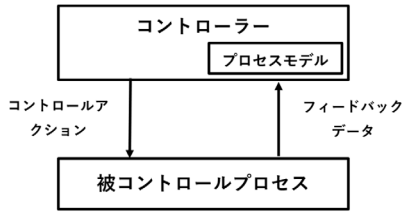
- 近年、サプライチェーンの脅威は増しており、リスクマネジメントは組織の内部だけでなく、委託先なども含めて実施する必要がある
- 2022年に尼崎市で委託先の従業員が個人情報を含むUSBメモリを紛失する事案が発生
  ⇒組織が包括的なリスクマネジメントを実施できていない可能性

その一方で、

- 従来の信頼性工学のリスクマネジメント手法は、システムの各構成要素に着目
  ⇒包括的なリスクマネジメントを実施するには、構成要素間の相互作用も考慮する必要がある
- 近年では、構成要素間の相互作用に着目した**STAMP/STPA**が注目されている

STAMP/STPAとは

- STAMP（アクシデントモデル）
  多くのシステム事故は、制御する側（コントローラー）と制御される側（被コントロールプロセス）の相互作用（コントロールアクションとフィードバックデータ）が働かない事によって起きる



- STPA（安全性解析手法）
  STAMPモデルを基にして、システムのリスク要因を特定する分析手法

STAMP/STPAの問題点

- STAMP/STPAはリスク要因を特定する際、ガイドワードを使用することでリスクを特定しやすくしている

1	コントロール入力や外部情報の誤りや喪失
2	不適切なコントロールアルゴリズム（作成時の欠陥，プロセスの変更，誤った修正や運用）
3	不整合，不完全，又は不正確なプロセスモデル，不正確な操作．
4	コンポーネントの不具合．経年による変化
5	不適切なフィードバック，あるいはフィードバックの喪失．フィードバックの遅れ．
6	不正確な情報の供給，又は情報の欠如．測定の不正確性．フィードバックの遅れ．
7	操作の遅れ．

- しかし、ガイドワードは機械やソフトウェア向けに作成されており、組織や社会的要因の分析が不十分になってしまう可能性
- IPA（情報処理推進機構）では、人・組織に対応したガイドワードが提案されているが、ヒューマンエラーに着目しているため、法令や不正を考慮できていない

研究目的

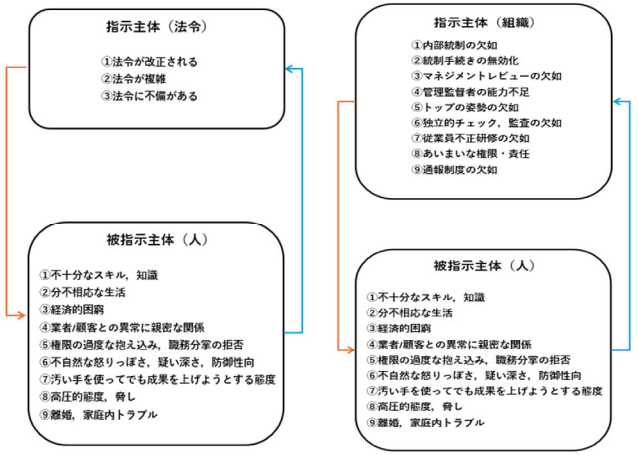
複雑で絡み合った複数の組織やシステムの安全性を向上させる

⇒STAMP分析を用いて包括的なリスクマネジメントを実施できることを目標とする

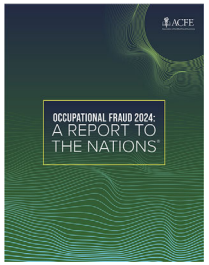
研究方法

1. STAMP分析のリスク要因（HCF)を特定するためのガイドワードを新たに作成する
2. 尼崎市のUSBメモリ紛失事案を分析対象として、STAMP分析を実施する。その際、IPAが提案しているガイドワードと新たに作成したガイドワードをそれぞれ適用する
3. IPAが提案しているガイドワードと新たに作成したガイドワードを適用した結果を比較し、提案手法の有効性を考察する

新たに作成したガイドワード

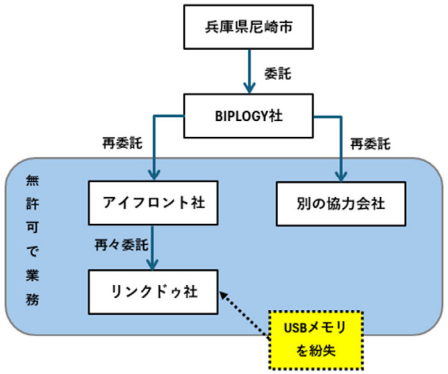


- 日本公認不正検査士協会の調査を基にガイドワードを作成



▲職業上の不正に関する国民への報告書

分析対象（尼崎市USBメモリ紛失事案）について

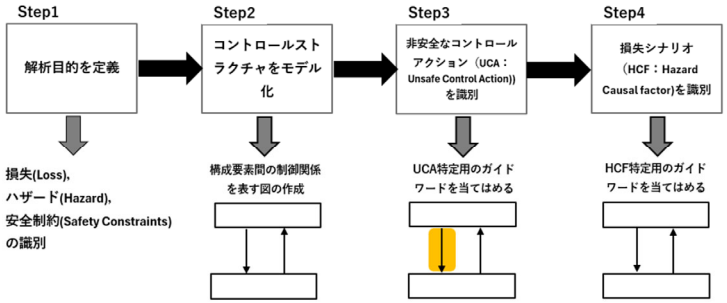


- 事件の概要
  - 尼崎市が、住民税非課税世帯等に対する臨時特別給付金支給対応業務における業務をBIPLOGY株式会社に委託した。この業務は無許可で再委託、再々委託された。
  - 同社の再々委託先従業員はコールセンターでのデータ移管作業のため、住民の個人情報を含むUSBメモリを持ち出した。
  - データ移管作業終了後、飲食店で飲食し、帰宅時にUSBメモリを紛失する事案が発生した。

分析結果

尼崎市のUSBメモリ紛失事案を分析対象として、STAMP分析を適用した

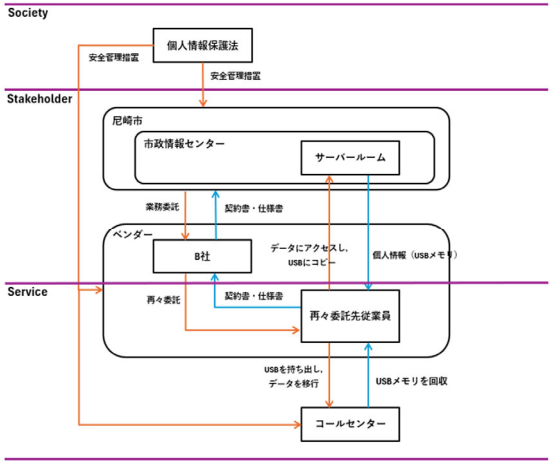
【分析手順】



Step1　解析目的を定義

アクシデント	ハザード	安全制約
(A1)市民の個人情報が流出する	(H1)個人情報の入った媒体を紛失する	(SC1)個人情報の入った媒体は厳重に管理されなければならない
(A1)市民の個人情報が流出する	(H2)無断で個人情報にアクセスされる	(SC2)無断で個人情報にアクセスされてはならない
行政サービスが停止する	サーバの設備，又はソフトウェアに障害が発生する	設備やソフトウェアは定期的にメンテナンスを行う
行政サービスが停止する	災害が発生し，業務の継続が困難になる	災害に備えて，バックアップ体制を整える

Step2　コントロールストラクチャをモデル化



- STAMP S&Sで使用される5階層モデルを取り入れて作成した。
- 5階層の内、下の2層（Software、System）に関しては、不明な点が多いため省略した。

Step3　非安全なコントロールアクション（UCA）の特定

	コントロールアクション	与えられないとハザード	与えられるとハザード	早すぎ，遅すぎ，誤順序でハザード	早すぎる停止，長すぎる適用でハザード
1	データにアクセスし，USBにコピー	データにアクセスすることができないため，個人情報が流出することはない	**(UCA1)無断でデータにアクセスし，USBにコピーする．（SC2違反）**	**(UCA1)許可を取る前にデータにアクセスし，USBにコピーする（SC2違反）**	特に重大な問題は発生しない
2	USBを持ち出し，データを移行	USBを持ち出せないため，データの移行はできないが，個人情報が流出することはない	**(UCA2)不適切な方法でUSBを持ち出す（SC1違反）**	特に重大な問題は発生しない	**(UCA5)USBを使い終えた後もUSBを返却しない（SC1違反）**
3	業務委託	業務委託が出来ない	**(UCA3)無断で業務委託し，許可されていない人が業務を行う（SC2違反）**	業務委託の契約が遅れる	特に重大な問題は発生しない
4	再々委託	業務委託が出来ない	**(UCA3)無断で業務委託し，許可されていない人が業務を行う（SC2違反）**	業務委託の契約が遅れる	特に重大な問題は発生しない
5	安全管理措置	個人情報保護法は制定されていると仮定するため，与えられないことはない	**(UCA4)不適切な安全管理措置を行う（SC1，2違反）**	特に重大な問題は発生しない	特に重大な問題は発生しない

Step4　損失シナリオ（HCF）の特定

・IPAが提案しているガイドワード

(UCA1)無断でデータにアクセスし，USBにコピーする．（SC2違反）	・データのアクセスに許可が必要だと思っていない．	・データのアクセスに許可が必要であることを忘れる．	・許可を取ったと勘違いしてデータにアクセスする．	・許可の取り方が分からない．	・業務を行う前にマニュアルを確認しない．
(UCA2)不適切な方法でUSBを持ち出す（SC1違反）	・適切な持ち出し方を知らない．	・セキュリティーの意識が低く，不適切な方法で持ち出す．	・体調不良や災害，事故などで適切な持ち出しができない．	・業務を行う前にマニュアルを確認しない．	
(UCA3)無断で業務委託し，許可されていない人が業務を行う（SC2違反）	・業務委託に関する基準が曖昧．	・担当者や責任者が不在で，誰って業務委託する．	・担当者が知識不足で契約内容を理解できずに業務委託をする．		
(UCA4)不適切な安全管理措置を行う（SC1，2違反）	・法令が改正し，基準や規則が変更される．	・法令が複雑なため，事業者が理解できない．	・新技術に法令が対応していない		
(UCA5)USBを使い終えた後もUSBを返却しない（SC1違反）	・コールセンターにUSBを忘れる．	・USBを返却することを忘れる．	・違う相手にUSBを返却する．	・USBを返却したと思い込む．	・体調不良や災害，事故などでUSBを返却できなくなる．

・新たに作成したガイドワード（一部）

(UCA1)無断でデータにアクセスし，USBにコピーする．（SC2違反）	・データにアクセスするのに許可が必要だと知らない．	・従業員が分不相応な生活をしており，お金に困っている．	・従業員が経済的に困窮している．	・市職員や他の協力会社と異常に親密な関係がある．	・担当者が仕事や責任を過度に抱え込んでいる．
(UCA2)不適切な方法でUSBを持ち出す（SC1違反）	・USBの適切な持ち出し方を知らない．	・従業員が分不相応な生活をしており，お金に困っている．	・従業員が経済的に困窮している．	・市職員や他の協力会社と異常に親密な関係がある．	・担当者が仕事や責任を過度に抱え込んでいる．
(UCA3)無断で業務委託し，許可されていない人が業務を行う（SC2違反）	・契約書や仕様書をチェックする体制が整っていない．	・組織内で情報共有できる体制が整っていない．	・業務契約を担当している者の能力が不足しており，業務委託をする．	・担当者や権限が曖昧で契約書をチェックする体制が整っていない．	
(UCA4)不適切な安全管理措置を行う（SC1，2違反）	・法令が改正し，基準や規則が変更される．	・法令が複雑なため，事業者が理解できない．	・法令に具体的な手法が明記されておらず，適切な措置が行えない．	・担当者の能力不足により，法令を理解できない．	・法令が守られているかのチェック体制がない．
(UCA5)USBを使い終えた後もUSBを返却しない（SC1違反）	・USBを返却することを知らない．	・従業員が分不相応な生活をしており，お金に困っている．	・従業員が経済的に困窮している．	・市職員や他の協力会社と異常に親密な関係がある．	・担当者が仕事や責任を過度に抱え込んでいる．

HCFの数（但し、同じHCFは1つとカウント）
- IPAが提案しているガイドワード：**20個**
- 新たに作成したガイドワード：**23個**

考察

IPAが提案しているガイドワードと新たに作成したガイドワードの適用結果を比較した

	IPAが提案しているガイドワード	新たに作成したガイドワード
法令	対応するガイドワードがないため，ガイドワードなしで分析する必要	ガイドワードを使ってHCFを特定することが可能
組織	ヒューマンファクターズに関するものが中心	組織の管理体制に関するものが中心
人	ヒューマンファクターズに関するものが中心	不正の動機に関するものが中心

- **提案手法は、不正に関する要因を多く特定することが可能。既存手法は、ヒューマンファクターズに関するものが多い**
- **提案手法がすべての分野において有効性があるわけではない**

まとめ

【結論】
- 新たに作成したガイドワードは不正に関しては十分な有効性がある。しかし、IPAのガイドワードで分析できていたヒューマンファクターズに関する要因は不十分

→状況に応じて使い分けることが重要

【今後の課題】
- 一部のガイドワードは当てはめてもリスク要因を特定できなかったため、より理解しやすい表現に変更するなどの改良が必要

付録

事例（尼崎市）について

- 尼崎市の事例では再々委託先従業員に悪意があったわけではなかったが、今回作成したガイドワードを適用することによって、悪意がない事例においても一定の有効性があると考えられる。