L-020

システム監査における ATT&CK フレームワークに基づく不正検知手法の提案

A Proposal of Fraud Detection Methods Based on ATT&CK Framework for System Auditing

郷田 大造† 島 成佳† 松井 亮宏‡
Taizo Goda Shigeyoshi Shima Akihiro Matsui

1. はじめに

DX の進展により，企業などの組織において IT システムを用いた業務や運営を行うことが一般的になった．組織において複数の IT システムを使って業務を行うようになり，組織における IT システムへの依存度・重要度は高まっている．IT システムへの依存度・重要度の高まりによって，IT システムが適切に運用され，リスク管理がされているのか客観的に評価するシステム監査の重要性が増している．監査人は，IT システムを評価するため，システムのログなどを確認することで，組織の IT システムが適切に運用されているのか評価している．

システム監査業務には，適切に IT システムが運用されていることを監査するため，仮説（帰無仮説）を用いて監査を行うものがある． 仮説を用いた監査において， 監査人が IT システムを用いた不正（以降，不正と呼称）を検出する精度にはバラツキが生じている．バラツキの原因は以下の２つである．

- 監査人ごとの監査経験の差
- 監査経験の共有量の差

本研究は，不正検出精度のバラツキに関する課題において，課題の解決方法となるフレームワークと，フレームワークを元に，不正検出業務を効率化・自動化する手法の提案を行う．本論文では，手法の元になるフレームワークについて提案を行う．本論文の構成は，2 節で課題分析を行い，3 節で課題解決のアプローチ方法について述べる．4 節で課題解決方法を述べた後解決方法が有効か確認し，5 節で確認結果の考察を述べ，6 節でまとめを述べる．

2. 課題分析

システム監査では，適切に IT システムが運用されていることを確認するため，帰無仮説を用いた監査が行われている．帰無仮説を用いた監査というのは，不正が行われたという仮説のもとシナリオを作成し，そのシナリオに沿って IT システムを監査するというものである．シナリオに沿って監査を行った結果，不正が見つからなければ，不正は行われていないということを証明できる．しかし，監査に用いるシナリオは監査人ごとに異なっており，不正検出精度のバラツキを生んでいる．筆者らは，この課題を分析して，考えられる原因を監査人にインタビューし，原因を明らかにした．以下では，バラツキを生んでいる 2 つの原因の説明を行う．

- 監査人ごとの監査経験の差

個々の監査人が体験してきた監査経験（以降，経験と呼称）は，異なっておりその経験量に差がある．経験の乏しい監査人よりも，経験が豊富な監査人の方がシナリオ作成する能力が高いため，不正の検出につながる．それは，経験豊富な監査人は，様々な監査を通して，不正のパターンや特徴を理解しており，不正とシステム，業務などの事柄を関連付けたシナリオを作成できるからである．

- 監査経験の共有量の差

監査人ごとの経験の差の他に，他の監査人から共有された経験の量には差がある．共有を受けた経験の量が多い監査人は，少ない監査人と比べ，自分の経験の他に共有された経験を活かして網羅性が高いシナリオを作成できるため，不正の検出につながる．

監査人ごとの経験の差と，経験の共有量の差が検出精度のバラツキに繋がっていると考える．次節では，2 つの経験の差によって生じている，バラツキを改善するためのアプローチ方法について述べる．

3. 課題解決のアプローチ方法

前節で課題分析を行ったところ，課題の原因は，監査人ごとの経験の差と，経験の共有量の差によるものであることが明らかになった．これらの課題解決のため，MITRE ATT&CK フレームワーク[1]（以降，ATT&CK と呼称）をベースにすることが有効である．以下にその理由を述べる．

年々不正は，単一のシステムや手法を利用したものだけでなく，複数のシステムや手法を活用した不正になりつつあり複雑化している．複雑化している不正に対処するため，監査人の垣根を超えた経験共有を行うことが必要である．

不正と同様に複雑化し，対処が困難になっているものとして，サイバー攻撃がある．サイバー攻撃では，ATT&CK をベースに経験を共有することで，複雑化に対処している．不正においても，ATT&CK と同様の仕組みのフレームワークがあれば，不正に対処できると考える．また，不正におけるフレームワークには，ATT&CK をベースとすることができると考える．それは，不正は IT システムを用いて内部から不正が行われており，IT システムを目的とした内部からのサイバー攻撃であると考えられるからである．方向の違いはあれど，IT システムを目的としている部分は同じであるため，ATT&CK をベースにしたフレームワークが不正に対して有効に働くと考える．次節では，不正に対処するためのフレームワーク（以降，監査フレームワークと呼称）のベースを ATT&CK とすることが有効か確認し，結果を述べる．

[1] https://attack.mitre.org/

† 長崎県立大学 University of Nagasaki
‡ ISACA 大阪支部／株式会社メトリックス
ISACA Osaka Chapter/Metrics,Inc.

4. 課題解決方法と確認結果

ATT&CK は，複雑化するサイバー攻撃を戦術や技術などに分解して，体系的にまとめているフレームワークである．ATT&CK の戦術とは，IT システムを狙ったサイバー攻撃のライフサイクルを攻撃者の目的ごとに 14 の段階で分解したものである．他方，技術は戦術の目的を達成するための手法のことである．ATT&CK が戦術や技術を体系的にまとめていることによって，サイバー攻撃を戦術と手法の面から理解することができ，攻撃に対して網羅性が高い対処を行えるようになった．

以下では，監査フレームワーク作成に向け，ベースとして ATT&CK が有効になるか確認し，課題の抽出を行う．課題抽出は，ATT&CK が不正ではなくサイバー攻撃を対象に作成されていることから，ATT&CK が不正についてどこまで適用でき，何が適用できないのか確認するために行う．

確認は，筆者らが考案した簡易的な事例について以下の手順で行うものとする．

1. 事例を戦術ごとに適用し適用できたら○を付す
2. 事例を技術に適用し適用できたら技術名を記述する

確認の結果をまとめたのが表 1 である．表 1 の左側には，ATT&CK の戦術を記述し，表の上側は戦術，技術としている．戦術は，事例を適用できた戦術に「○」を付し，できなかったものは「／」を付している．技術は，適用できた技術においては，技術名を記述し，できなかったものは「なし」としている．

表 1：簡易的な事例を ATT&CK に適用した結果

事例： 社員 A が事前に把握済み(1)の機密ファイルが保管されているサーバに，社員 A の認証情報を使いログイン(3)し，ファイルを自端末にダウンロード(4)(5)する．ダウンロード終了後，自端末から用意した USB にコピー(2)(6)して社外に持ち出す		
戦術 （適用できたものに○をつける）		**技術** （適用できた技術名を記述する）
Reconnaissance (1)	○	Search Open Website/Domains
Resource Development (2)	○	なし
Initial Access (3)	○	Valid Accounts
Execution	／	なし
Persistence	／	なし
Privilege Escalation	／	なし
Defense Evasion	／	なし
Credential Access	／	なし
Discovery (4)	○	File and Directory Discovery
Lateral Movement	／	なし
Collection (5)	○	Data from Local System,
Command and Control	／	なし
Exfiltration (6)	○	Exfiltration Over Physical Medium
Impact	／	なし

表 1 のように．一部の戦術と技術では，ATT&CK を適用できた．次節では，表 1 の結果を元に考察を述べる．

5. 考察

前節では，事例を適用することで，ATT&CK の戦術や技術における適用の可不可が明らかになった．以降では，適用の可不可の理由についてそれぞれ考察を行う．

筆者らが考案した事例では，一部の戦術や技術を ATT&CK に適用できた．ATT&CK で定義されている 14 の戦術は，IT システムを狙った外部から内部へのサイバー攻撃のライフサイクルを分解したものであるが，「IT システムを狙った攻撃」という部分は，不正においても変わらないため一部の戦術や技術を適用できたと考える．

適用できなかった戦術や技術については，ATT&CK の対象が関係していると考える．ATT&CK の対象は，サイバー攻撃であり，外部から内部に向かっての攻撃を想定している．しかし，不正は内部から内部に向かって攻撃を行うものが多い．また，不正は社員など組織が信用している組織内の人間が行うものもあり，外部から外部の人間による攻撃を想定している ATT&CK の戦術や技術に適用することが難しかったと考える． 監査フレームワーク作成のため，ATT&CK で対応できていない，内部から内部を対象とした攻撃という観点で戦術や技術を変更・追加する必要があると考える．また，今後実際の不正事例を ATT&CK に適用し，適用の可不可や適用判断に迷う部分を改めて明らかにする必要がある．不正事例を元に，適用が困難または，適用の判断に迷う戦術や技術については，新たに定義する必要があると考える．

6. まとめ

本論文では，監査人が行うシナリオを用いた監査において，不正検出の精度にバラツキが生じているという課題に対し分析を行い，課題の解決方法を提案した．課題分析の結果バラツキを生む原因として，監査経験の差，監査経験の共有量の差という 2 つが明らかになった．課題解決のため，ATT&CK をベースとした監査フレームワークの提案を行った．ATT&CK がベースとなることを確認するため，簡易的な不正事例を元に ATT&CK への適用を行い，一部適用できることを確認した．今後は，適用の可不可や判断に迷う部分の調査をすすめるため，不正事例を調査・収集し，ATT&CK への適用を進めたい．

参考文献

[1] 島田裕次：内部監査における不正リスクへの対応 ～システム監査を含めて～，現代監査，Vol.2014，No.24，pp.92-102（2014）．