コロナ禍における Know Your Employeeの効用

全世界的なコロナ禍によって、従来のオフィス業務は、テレワークへ移行しており、ポストコロナにおいてもこの傾向は継続するだろう。しかし在宅勤務では、周りに上司や同僚の目がないことによる内部不正の可能性など懸念も多い。その対策として既に英米で取組まれている従業員の行動監視（KYE）が有効と考える。

従業員の行動監視KYEの必要性

コロナ禍のテレワーク環境において、コンプライアンス部門による従業員の行動監視（KYE：Know Your Employee）が改めて注目されている。

在宅勤務中の従業員においては、周りに牽制機能としての上司や同僚からの目がなく、また会社側においては不慣れなリモート環境での業務運営に対する統制機能の不備など抜け漏れが生じる可能性もある。このような状況が重なると内部不正を誘発[1)]しやすい状態を生成すると言われている。また、ここで言う内部不正には、1）金銭搾取や横領などの内部犯罪、2）適合性原則違反や説明義務違反など顧客に対するコンプライアンス違反、さらには3）サボタージュ（勤怠不良）や業務命令に反する行為などの服務規程違反が含まれる。

このような新たな内部不正の発生リスクをチェックするために、“リモート環境に適した従業員のモニタリング”（以後、従業員モニタリングと呼ぶ）の仕組みを整備することが必要になってくる。従業員モニタリングは、在宅勤務などリモート環境における内部不正の防止に有効であるばかりでなく、テレワーク生産性[2)]を向上させたり、さらには顧客のニーズや嗜好などをより正確に把握できる効果（NBA：Next Best Action）も期待できる。日本ではまだ手付かずの従業員モニタリングについて、参考となる先行事例を紹介したい。

英米における不正防止監視の先行事例

現在、英国の金融機関においては、MiFID Ⅱ（Markets in Financial Instruments Directive Ⅱ：第2次金融商品市場指令）による金融商品販売時の説明記録、MAR（Market Abuse Regulation：市場濫用規制）におけるインサイダー対策用の行動記録、そしてEMIR（European Market Infrastructure Regulation：欧州市場インフラ規制）によるデリバティブ市場の取引関連データの報告、がそれぞれ義務化されている。そのため、各金融機関では営業担当者による顧客のあらゆる取引のデータ監視をするため、それに伴う顧客との通話音声やメッセージの保管・分析、さらに注文データや取引データ、日々の市場データに至るまで広範なデータを長期保管・分析している。まさにコンプライアンス違反監視の典型的な手法例と言える。

ちなみに日本においては、例えばコールセンターなど一部業務においてデータ（通話音声など）保管されているものの、すべての業務においてデータの保管・分析が行われているわけではない。

一方、米国では、内部犯罪の防止に重きを置いた従業員モニタリングの先行事例が見られる。図表の通り、金融機関1社平均で年間23件の内部不正が発覚しており、その対応コストは1社で年間11.45億円にまで膨れあがっている。このような状況を懸念してか、米国金融機関では内部犯罪の防止を意識した、様々な従業員モニタリングのツールを導入している[3)]。その機能は多様であ

図表　世界の有力企業における内部不正の被害実態

内部不正事件のあった世界の有力企業204社調査（2019年Q2）		
1社あたり平均年間発生件数		23件/年
年間損失コスト合計	過失	4.58億円/年
	犯罪	4.08億円/年
	情報漏洩	2.79億円/年
	総計	11.45億円/年

（出所）2020 Cost of Insider Threats Global Report

NOTE

1) 米国の社会学者であるDonald Ray Cresseyは、組織の内部者が不正に至る3つの要因（機会・動機・正当化）を定義し「不正のトライアングル（fraud triangle）」と呼んだ。
2) 業務の生産性を向上させるには、「デジタル化」が最も効果的な対応だと言われているが、本論では“リモート環境”での生産性の課題に特化させるため「デジタル化」の議論は対象外とする。
3) 米国では、会社として従業員に黙ってモニタリングすることは禁止されており、例えばコネチカットやデラウェアなどの州では、労働法により「従業員に対して、事前にモニタリングする旨を通知すること」を義務付けている。（Delaware Code TITLE 19 Labor General Provisions CHAPTER 7. Employment Practices §705(b)(2) “Has first given a 1-time notice to the employee of such monitoring or intercepting activity or policies.”）。
また、カリフォルニアやイリノイなどの州では、通信傍受法により「電子メールのすべての当事者に傍受の同意を得ること」を義務付けている。つまり、外部との送受信の場合、外部の第三者にも同意を得なければならないことになる。
4) “Gartner Identifies Nine Trends for HR Leaders That Will Impact the Future of Work After the Coronavirus Pandemic”, May 6, 2020, Gartner (https://www.gartner.com/en/newsroom/press-releases/2020-05-06-gartner-identifies-nine-trends-for-hr-leaders-that-wi)

り、例えば、従業員のメールやメッセンジャーを監視・保管するツールや、PC内にダウンロードしたデータや送信中のデータの中身を監視するツール、さらにはシステム操作ログや画面のスクリーンショットの取得、挙句にはPC内臓カメラが自動で立ち上がり、業務中の従業員の姿を監視するものまで存在している。

また、Gartnerの調査[4]によると、米国ではコロナの流行以前から全米就労者の約30%が既にリモート勤務しており、約16%の企業がなんらかの従業員モニタリングツールを活用して従業員の行動監視を実施している。そしてパンデミック後には74%の企業がリモート勤務の増加を計画しており、従業員モニタリングを行っている企業の割合も、ますます増加傾向にあるとされている。

従業員モニタリングを構成する『3つの機能』

従業員モニタリングは大きく3つのソリューションカテゴリーに分けられ、それぞれ機能的役割があると考えている。

1つはプロセスマイニングである。プロセスマイニングは、従業員が会社貸与のPCを使用して業務を行う際に、すべての操作を記録する機能である。これにより、従業員の業務を正確に再現することが可能であり、万が一の内部不正の発生に対して、その行動履歴を確認することができる。また、社内規程に抵触する不正なファイルアクセスなどのリアルタイムでの監視も可能だ。

2つ目は、会社貸与の携帯電話などによって、顧客との営業対話を行った記録の分析である。音声のまま、あるいはテキスト化した文章を分析し、コンプライアンスの確認や不正の可能性を秘めた会話など調査することができる。

3つ目は、不正発生の予兆把握である。取引データや入出金データなど関連するデータ群と、上記のプロセスマイニングや通話記録分析の結果などを組み合わせて機械学習させたAIモデルにより、“過去の通常の取引行動とは異なる動き（不正予兆の可能性）”を検知する仕組みである。

“攻めと守り”の従業員モニタリング実現に向けて

さて、日本ではテレワークは始まったばかりだが、このようなリモート環境における従業員モニタリングの仕組みが整備されないままでは、従来のオフィス勤務と同等の重要業務（機微情報を含む秘匿性の高い基幹業務など）を安心して在宅勤務に任せることはできない。かといって重要度の低い単純業務だけ任せても業務生産性は低く、実質は自宅待機となる状態を生み出しかねない。

積極的に従業員モニタリングを導入し、“守り”としての『3つの機能』を整備することで、“攻め”としての重要度の高い基幹業務を在宅勤務でも実施できる、高い生産性を得られるリモート環境を構築すべきと考える。また、リモート環境だからこそ得られる顧客に関する大量の取引データや対話データなどから顧客嗜好などの解析も可能と考えている。これらの“攻・守”の整備により、テレワークが増加した状況下でも、変わらぬ企業競争力を維持することができるだろう。

Writer's Profile

小林 孝明 Takaaki Kobayashi
金融デジタル企画一部
上級研究員
専門はリスク管理、AML、金融サスティナブル研究等
focus@nri.co.jp