

LPM より「内部不正を見抜く方法」 How to Detect Internal Dishonesty

By: Cory Lowe, PhD & John Matas, CFE, CFCI

February 11, 2026

☆このレポートの中で学びたいポイント

1. 背景（内部不正が軽視されがちである理由）
2. 不正の発生メカニズム（動機・機会・監督）
3. 組織文化とリスク要因
4. 検出手法
①教育、②RFID、③匿名通報、④EBR、⑤監査

過去5年間、小売業者は、他の犯罪や悪質な商品損失の原因よりも、暴力と ORC（組織的小売犯罪）に対する懸念を公に表明してきました。しかしながら、従業員による不正行為が減少していると判断できる根拠は見当たりません。むしろ、取引や配送、販売チャネルの拡大により、不正行為の機会はむしろ増えており、状況は悪化していると考えられます。

しかしながら、内部不正は ORC や暴力犯罪ほど注目を集めていません。これは、単に深刻な問題ではないからというだけではありません。暴力と ORC は、単に目に見えるという理由から、より大きな注目を集めているのかもしれませんが、場合によっては、これらの犯罪は、小売業者、法執行機関、その他の利害関係者間の外部的な協力をより必要とするため、より「目に見える」ものとなる可能性があります。内部不正は、多くの場合、他の利害関係者との広範な協力なしに対処できるため、公に非難する理由は少なくなります。言い換えれば、小売業者は、従業員による不正行為に対して、他の犯罪よりも大きな影響力を行使できることが多いのです。

本稿では、小売業者が内部不正をより効果的に検知するために活用できる手法について考察します。これは、内部損失の規模と、それが全体の損失に占める割合を推定するための最初のステップとして不可欠です。大きな可能性を秘めている事例としては、例外ベースの報告（EBR）といった従来の慣行に新たな工夫を凝らすことや、コンピュータービジョンや無線周波数識別（RFID）といった技術を活用することが挙げられます。しかし、業界内の他の問題と同様に、内部不正は一律に発生するわけではありません。店舗の立地、店舗内のエリア、その他リスク要因は多岐にわたります。効率性の観点から、小売業者はリスクが最も高い分野に予防、検知、その他の管理策を集中させることが重要です。

基本を理解する：従業員が犯罪を犯す理由

リスクを対象としたプログラムを構築するためには、従業員がなぜ不正を行うのかを理解することが重要です。ここでいう「従業員がなぜ不正を行うのか」とは、彼らの動機や、犯罪によって何を達成しようとしているかという意味ではありません。むしろ、従業員の不正行為や犯罪の「原因」について指しています。

従業員による窃盗、詐欺、その他の不正行為は、一般的にいくつかの主要な要因に集約されます。それは、動機、犯罪傾向（犯罪を行う性質）、そして機会です。

- ・動機と傾向には、同様の機会があった場合に犯罪を犯す可能性における個人差に影響を与えるあらゆる要因が含まれます。これには、経済的ストレス、犯罪を助長する信念、過小評価されていると感じること、不当な扱いを受けていると感じることなど、様々な要因が含まれます。

- ・犯罪を犯す機会には、防御策のあらゆる弱点が含まれます。言い換えれば、機会こそが、動機の強い個人が、摘発や結果のリスクを最小限に抑えながら犯罪を犯す可能性を与えるものなのです。

- ・監督は重要な要素であり、多くの小売業のリーダーは、従業員による窃盗や詐欺行為はすべて監督の不備であると言うでしょう。

したがって、犯罪は動機や性向、そして機会が存在する場合に発生すると考えられます。犯罪を犯す機会があっても、性向や動機がない場合、犯罪は起こりにくいと考えられます。逆に、犯罪を犯す動機や性向はあるものの、刑務所に収監されている場合、多くの種類の犯罪に手を染める機会は失われます。

こうした現実には、従業員による犯罪の摘発に深刻な影響を及ぼします。動機と犯罪性向が人口全体に均等に分布していると仮定した場合（実際にはそうではありません）、より多くの機会を持つ従業員の犯罪発生率が高くなると予想されます。例えば、現金を直接扱ったり、経理業務に従事したりする従業員は、現金窃盗や横領の発生率が高いと予想されます。逆に、機会が均等に分布している場合、動機や性向がより高い従業員の犯罪発生率が高くなると予想されます。

一方で、従業員は非従業員に比べて犯罪を行う機会が多いという点がいくつかあります。第一に、外部の犯罪者は小売店舗に行くために特別に足を運ぶ必要がありますが、小売従業員は仕事としてそこに常にいます。

従業員は、店舗運営の中核にアクセスできる立場にあります。仕事の一環として、通常の防御手段を迂回できる権限が与えられています。

第三に、従業員は防犯措置や手順に精通しており、それをいかに回避するかについて、外部者よりも理解している可能性があります。

さらに、従業員は非従業員と接触するため、共犯が生じる独特の機会が生まれます。つまり、内部の関係者が外部の、顔見知りではない者を支援し、犯罪の実行を手助けすることがあり、その結果、犯罪の発見・捜査・管理がより困難になります。

これは特に、脅迫や報酬によって従業員をリクルートする ORC グループにおいて顕著な問題です。

こうした理由から、従業員の監督と内部統制は、従業員による犯罪を防止するうえで極めて重要なのです。

こうして考えると、小売業者にとって状況は厳しいように思えるかもしれない。しかし、外部からの犯罪にはない、従業員の不正行為を防止、検知、対処するための機会には他にも存在する。第一に、従業員による犯罪の種類によっては、小売業者が導入できる具体的な管理策があり、監督と監視のための独自の機会が存在する。たとえば、LP プログラムは、勤務スケジュール、POS 取引データ、監視映像など、従業員の違反行為に関連するより多くのデータを分析できます。

しかし、もう一つの利点は、多くの非従業員犯罪とは異なり、小売業者には犯罪の機会を制限する以上の選択肢があるということです。非従業員の場合、小売業者が犯罪の動機や傾向に影響を与えるためにできることは限られています。場合によっては、LP プログラムやその他の事業部門が、従業員の犯罪に寄与する個人的および社会的要因に対処できる可能性があります。

研究者たちは、従業員犯罪全般、特に小売業従業員の犯罪に関連する多くの個人的および社会的要因を発見しました。従業員の不正行為のリスク要因には、仕事への満足度とコミットメントの低さ、経営陣への不満、経済的困難、不公平感の認識、監督の欠如、長期的な雇用見通しの低さ、犯罪に協力的な同僚や社会の影響、自制心の低さ、そして仕事への不満にも関連する職場の自律性の低さなどが挙げられます。これらのリスク要因はすべて、理論的には、個人的なストレスや緊張、社会的影响、そして雇用主を犠牲にしても失うものがほとんどない、あるいは全くないという従業員の気持ちが絡んでいるという点で、他の多くの種類の犯罪と同様です。

個人が犯罪を助長する態度、信念、知識（例えば、犯罪のやり方）を持っている場合、そうした行動に手を染める可能性が高くなります。小売業者が明確な規範や行動基準を持たず、非倫理的な行動を放置したり、店舗内で犯罪的な態度に対処できなかつたりすると、内部損失に苦しむ可能性があります。個人的なストレスや緊張については、小売業者には、労働条件の管理や、困難な時期に従業員を支援すること（従業員支援プログラムな

ど) など、これらのプレッシャーを軽減する選択肢があります。

企業文化は非常に重要であり、経営陣によって構築・維持されなければなりません。従業員が(「お気に入り」の個人に対してであれ、より一般的にであれ)手抜きや非倫理的な行動が容認されていると認識すると、不正行為が常態化する可能性があります。不正行為や暴力は明白であり、しばしば報告されますが、従業員による犯罪の多くは、はるかに目立ちにくいものです。したがって、内部不正は報告された時点で対処し、そのまま放置されないようにすることが重要です。報告を奨励し、内部不正を抑制する企業文化を確立することは重要ですが、小売業者が高圧的になりすぎると、意図しない影響が生じる可能性があります。この場合、小売業者は不信感を醸成する文化を作り出し、従業員の離反や不満を生み、内部不正を悪化させる可能性があります。その結果、従業員は自らの不正行為を正当化しようとします。例えば、従業員は「雇用主は私を信頼しておらず、気にかけてもいないのに、なぜ私が雇用主を気かけなければならないのか?」と自問し始めるかもしれません。

小売業者は、組織全体にわたってこれらのリスク要因に関するデータを収集することで、社内不正の検出を含む従業員の犯罪対策に注力することができます。小売業者は、アンケート調査、離職率データ、従業員エンゲージメントおよび感情データを社内リスク分析の一環として活用できます。例えば、士気が低く離職率の高い店舗は、社内不正のリスクが高い可能性があります。

小売業者は、店舗レベルおよび個人レベルでリスク要因に影響を与えるために多くの対策を講じることができます。また、監督と監視を強化し、追加の管理策やプロセスを導入することで、従業員の犯罪機会を制限する方法も数多くあります。フロリダ大学のロスプリベンション研究評議会(LPRC)の活動の多くは、状況犯罪予防の原則に基づいています。状況犯罪予防とは、状況や環境を修正することで、犯罪者の犯罪コストを増加させ、犯罪による利益を減少させることができることを示唆しています。小売業者が講じることができる重要な対策は3つあります。

- (1) 従業員が会社を被害者にする不正行為を実行するための負担を増やすことのために必要な労力を増やすこと、
- (2) 不正行為を実行するための負担を増やすこと(解雇や刑事訴追を含む懲戒処分の可能性など)を高めること、
- (3) 犯罪による利益を減らすことです。

小売業者が導入できる多くの摘発措置は、犯罪行為をより困難にし、従業員が雇用主を被害者にするもののリスクを高めるでしょう。

従業員の不正行為を検出するためのテクノロジー、プロセス、そして実践

幸いなことに、小売業者が従業員の不正行為を検出する方法は数多くあり、その多くは業界で広く知られています。しかし、思慮深く戦略的なアプローチを維持しながら、大規模な課題に対応できるプログラムを構築することは非常に困難です。このセクションでは、従業員の不正行為を検出するための様々な手法を概説します。しかし、小売業者は、いくつかのアイデアを選び、「問題に解決策を突きつける」だけでは成功を期待すべきではありません。LP チームは、従業員の不正行為を様々な方法で検出・抑制するための、一貫性のある階層化されたプログラムを構築する必要があります。これは、採用基準、人員、プロセス、トレーニング、そしてテクノロジー戦略を、リスクが最も高い領域に焦点を当てて、慎重に活用することを意味します。前述のように、内部不正の機会が多く、従業員の不正行為の動機や傾向が高い場合、リスクは最も高くなります。

教育、意識向上、そしてトレーニング

教育、トレーニング、そして意識向上は、あらゆるプログラムにおいて重要な要素です。適切に実施すれば、従業員の違反行為を検知するチーム全体の能力を高め、既存のプログラムへの意識向上にもつながります。プログラムを導入することは重要ですが、従業員の違反行為に対してプログラムが最大限の効果を発揮するには、従業員がそれを認識している必要があります。例えば、社内不正行為の調査に専念する調査チームがいても、従業員がそれに気づいていなければ、抑止効果は限定的なものになってしまいます。

研修と意識向上には課題とリスクが伴います。一方で、教育、研修、意識向上が慎重に設計されていない場合、逆効果になる可能性があります。例えば、小売業者が適切に設計されていない場合、従業員に雇用主を巧妙に利用する機会や、管理体制や LP プログラムにおける実際の、あるいは潜在的な脆弱性を認識させる可能性があります。さらに、教育と研修が強引すぎると、従業員を非難したり、不信感を抱かせたりする印象を与える可能性があります。同様に、離職率の上昇や違反行為の形態の急速な変化に直面しながら、従業員の研修を維持するという現実的な課題もあります。一方、トレーニングと意識啓発は、慎重に行われなければ、従業員が組織を搾取する機会に気付く可能性があります。

在庫・資産追跡

近年、在庫・資産追跡技術は飛躍的に進歩し、小売業者は内部不正をより正確かつ積極的に検知できるようになりました。従来の電子商品管理システム（EAS）は、特に目に見える抑止力として使用する場合、依然として有効ですが、他のシステムが提供するような情報を提供しません。EAS は、商品が店舗から持ち出されたことを識別できますが、どの商品が持ち出されたのか、合法的に販売されたのか、誰が持ち出したのかを確認することはできません。

RFID 技術は、これらの多くの限界を克服します。各商品に固有のコードを割り当てるこ

とで、小売業者は個々の商品を入荷から販売まで追跡できるだけでなく、店舗から持ち出された後に盗難品を特定することもできます。リーダーと取引データを統合することで、RFID システムは店舗から持ち出された商品を検知し、対応する売上があったかどうかを即座に判断できます。取引記録が存在しない場合は、特定の商品とタイムスタンプをフラグ付けして調査できます。この精度は、外部からの盗難と内部からの転用の両方を特定する上で非常に重要です。

RFID データは、店舗内の不一致を検出するためにも使用できます。例えば、高額商品が継続的に倉庫から出荷されるにもかかわらず、売場で補充されず、POS でも販売されない場合、その移動パターンは内部損失を示している可能性があります。同様に、POS で返品とマークされた商品は追跡調査によって、他の場所に流用されたのではなく、在庫に再投入されたことを確認できます。さらに、閉店前後に多くの商品が盗難される可能性があります。このような時間帯に商品がいつ店舗から出荷されるかを把握することは非常に重要です。

RFID の導入がまだ実現可能でない場合でも、従来の在庫管理手法は依然として不可欠です。高リスクカテゴリーでの頻繁なサイクルカウント、受領プロセスの監査、出荷差異の即時調整により、盗難や不正操作を検出できます。これらの従来の手法を在庫管理ソフトウェアやビデオ検証などのシステムと統合することで、損失活動をより深く理解することができます。つまり、効果的な在庫・資産追跡プログラムは、物理的な検証とデータインテリジェンスを組み合わせることで、損失の検出と可視性を確保します。

匿名報告

匿名報告プログラムは、内部不正を検出するための最も費用対効果が高く、かつ効果的な方法の一つです。これは、従業員が常に同僚と交流しているため、経営陣や他者よりも先に社内不正に気づく可能性が高いためです。しかし、こうしたプログラムの成功は、設計と徹底したフォロースルーに大きく左右されます。従業員が非倫理的または疑わしい行為を機密性を保ちながらアクセスしやすく、信頼できる方法で報告できる小売業者は、重大な損失につながるずっと前に問題を表面化させることができます。匿名報告システムには、サードパーティのホットライン、アプリ、従業員エリアに設置された報告フォームにリンクされた QR コードなど、さまざまな形態があります。昔ながらの方法で、従業員エリアに物理的な投函箱を設置することもできます。どの形態を選択するにせよ、従業員は自分の報告が適切な対応を取れる人物によって確認されていると確信する必要があります。

匿名報告は具体的な詳細が不足していることが多いですが、他のデータと組み合わせることで、貴重な方向性を示す情報を提供できます。複数の匿名の通報が同じ従業員、部門、

または行動パターンに言及している場合、これらの報告は、EBR、監査、またはビデオレビューの取り組みをどこに集中させるべきかを示唆します。効果的なプログラムは、情報が受け取られ、それに基づいて行動したことを認めることで、対応結果をフィードバックすることが重要です。行動を確実にすることは、従業員の参加を促す鍵となります。人々は、何らかの利益がある場合にのみ行動を起こします。利益がない場合、あるいは報告しても従業員が何の行動も起こさないと感じた場合、従業員がその行動を続ける理由はほとんどなくなり、問題は解決できます。

例外ベースのレポート

小売業者は膨大な取引データを保有しており、その量は増加の一途を辿っています。この現実の問題を引き起こす一方で、同時にその問題に対する便利な解決策も提供します。問題は取引量です。人間が手作業で確認するには量が多すぎるのです。しかし、大規模なデータセットを活用することで、「正常な行動」ではない、つまり異常な取引を特定することが可能になります。これが EBR の核心です。

適切に設計された EBR プログラムは、膨大な量の POS データと運用データを分析することで、無効、返品、割引、オーバーライド、そして通常とは異なる売上のない取引（つまり、標準からの例外）といった異常を特定できます。これらの活動に他の従業員よりも多く従事している従業員が 1 人または複数いる場合、特にチームメンバーがこれらの活動を増やす正当な理由がない場合は、懸念される可能性があります。例えば、監督者やマネージャーであれば、これらの活動にもっと多く従事することが期待されます。

最新の EBR プログラムは、他の形式のデータも取り込むことができ、さらなる検出と調査の機会を提供します。例えば、従業員のスケジュール、店舗のトラフィックデータなどの運用データ、その他様々な形式のデータを EBR プログラムに組み込むことができます。ビデオは例外の確認と検証に使用できますが、ビデオ分析の潜在的なユースケースは数多くあります。例えば、ゴミ捨て場の分析で、人々がゴミを出し入れする頻度を測定するとします。これは、業務上の非効率性や時間の浪費を検知できるだけでなく、ゴミ捨て場から商品を盗み取ろうとする人物も検知できます。同様に、従業員がレジ付近に私物バッグを置いているタイミングや、特定の行動や動作をどのくらいの頻度で行っているかを把握するためにも分析を使用できます。現在、人物検出や物体検出など、多くの基本的な分析機能が利用可能であり、ユースケースは今後も増え続けるでしょう。ある販売、取引、配送チャンネルのデータを使用して、別のチャンネルの異常な行動を検知できる、クロスチャンネル異常検知の機会はますます増えています。

EBR の意義の一つは、関連データを効果的に活用するためには、機械可読でアナリストがアクセス可能でなければならないということです。残念ながら、小売業では依然として多

くの手作業や手書きの記録、署名、数量、その他の重要なデータが関わっています。これらの記録がデジタル化されていないと、大規模な分析は不可能であり、EBRは不可能です。たとえデータがデジタル形式であっても、アクセスできない、または使用可能な形式になっていなければ、LPはデータを分析できません。例えば、特定の活動のデジタル記録は存在するかもしれませんが、容易にアクセスできるデータベースには存在しない可能性があります。

監査とレビュー

監査とレビューは、社内不正行為を検出するための不可欠なツールです。説明責任を明確にし、パターンを明らかにし、従業員による窃盗や不正行為を可能にする監督上の欠陥を明らかにします。例えば、アクセス制御ログを従業員のスケジュールやタイムキーピングデータと相互参照することで、レジ、倉庫、または立ち入り禁止区域への不正な立ち入りを特定できます。従業員が勤務時間外に、あるいは同様の職務を担う他の従業員よりもはるかに頻繁にセキュアスペースにアクセスしている場合、その行動を調査する必要があるかもしれません。ログイン監査は、もう一つの強力なツールとなります。POS ログインアクティビティとタイムレコーダーデータを比較することで、従業員が他人の認証情報を使用している可能性を明らかにできます。同様に、従業員の出勤時間と取引開始時間を比較することで、小規模ながらも一貫した時間窃盗のパターンを発見できます。

物理的な確認プロセスも見逃してはなりません。許可されている場合、一貫して丁寧に実施されるランダムな手荷物検査やロッカー検査は、窃盗と隠蔽の両方を抑止することができます。同様に、返金、無効、割引取引、特に通常のパターンから外れた取引を定期的に確認することで、一見正当に見える不正操作を明らかにすることができます。

プロセスコンプライアンス監査は、財務監査と同様に多くの情報を提供することができます。例えば、返金された商品が実際に棚に戻されているかを確認したり、現金の差異が適切に文書化されエスカレーションされているかを確認したりすることで、不正行為だけでなく、プログラムの脆弱性も明らかにすることができます。優れた監査プログラムは、例外報告、店舗業績、過去のインシデントなどを通じて特定されたリスク領域に焦点を当てます。つまり、不正行為の可能性が最も高い領域にリソースを確実に配分します。したがって、柔軟性リスクの変化に応じて焦点を調整できる柔軟性を備えたプログラムが不可欠です。

結論：リスクベースの検出

結局のところ、内部不正を検出する最良の方法は、リスクに合わせてカスタマイズされたソリューションと戦略を活用することです。この記事では、従業員の不正行為の既知のリスク要因とその検出方法について説明しました。LPプログラムを最大限に効率的にするた

めに、小売業者は課題に直面する可能性が最も高い領域を評価し、ソリューションと戦略を展開する必要があります。

出典 <https://losspreventionmedia.com/how-to-detect-internal-dishonesty/>

翻訳 2026年2月19日 工業会 JEAS（稲本/CFE 公認不正検査士）

この内容は工業会 JEAS のロス対策メルマガ（<https://www.jeas.gr.jp/mail.html>）2026年04月22日 12:00 に配信されます。

以上