Information-technology
Promotion
Agency, Japan

第 14-04-310 号
2014 年 3 月 4 日
独立行政法人情報処理推進機構

今月の呼びかけ

経営者・マネジメント層向け
「 組織内部の不正行為にはトップダウンで、組織横断の取り組みを 」
～現状チェックと対策ポイントの見直しで効果的に内部不正を防止～

2014 年に入り、金融機関や行政機関において業務に携わる者による情報窃取等の不正行為の報道がありました。

このように不正行為は、従業員や委託先社員等の組織の内部情報にアクセスできる関係者（以後、内部者）によって行われることがあり、その多くは金銭やビジネス利用等を目的としています。

米国の調査※1には、その経済的な影響について、内部者による不正行為は、外部からの攻撃に比べて発生件数は少ないが、その被害額は同等かそれ以上という結果があります。そのため、**経営層は、そのリーダーシップのもと、各部門を横断的に密連携させ、委託先も含めた内部不正対策に取り組む必要があります。**しかし、前例に学ぼうとしても被害にあった組織は信頼や評判が損なわれるといった負の影響を懸念し、情報が公表されることはまれで、その実態を把握しにくいのも事実です※2。

そこで今月の呼びかけでは、2013 年 3 月に公開した「組織における内部不正防止ガイドライン」をもとに内部不正を防止するための対策を説明します。

※1　2013 U.S. State of Cybercrime Survey
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=58738
※2　IPA：「組織内部者の不正行為によるインシデント調査」を参照
http://www.ipa.go.jp/security/fy23/reports/insider/index.html

（１） 内部不正を防止するための現状把握と対策の検討

IPA では、内部不正による事故・事件の発生を防止するための環境整備に役立つよう、2013 年 3 月に「組織における内部不正防止ガイドライン※3」（以下、ガイドライン）を策定し、公開しています。

ガイドラインでは基本方針や技術的管理、人的管理、物理的管理など 10 の観点から 30 の対策項目を示しています（図 1 参照）。

ガイドラインを効果的に活用するには、最初にチェックシートで対策の現状を把握し、次に、その結果を基に必要な対策項目を検討します（図 2、3 参照）。具体的な実施策の検討には、各対策に必要な製品、ソリューションが紹介された、日本ネットワークセキュリティ協会（JNSA）の「内部不正対策ソリューションガイド※4」が参考になります。

	経営者	情報システム部	総務部	人事部	法務・知財部	営業・開発等の各部門
1.基本方針	○					
2.資産管理		○				○
3.物理的管理		○	○			○
4.技術的管理		○				○
5.証拠確保		○				○
6.人的管理			○	○	○	○
7.コンプライアンス			○	○	○	○
8.職場環境			○	○		○
9.事後対策		○				○
10.組織の管理		○				○

図 1：内部不正対策の 10 分類と関連部門

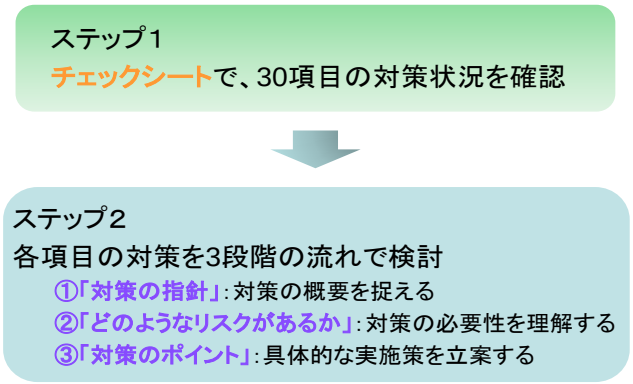

図 2：内部不正防止ガイドラインによる対策検討の流れ

No	内容	チェック欄
4-1. 基本方針		
(1)	内部不正の対策が経営者の責任であることを組織内外に示す「基本方針」を策定し、役職員に周知徹底していますか?	□:経営者(最高責任者)
(2)-①	経営者は、内部不正対策の総括責任者の任命及び管理体制と実施策の承認を行っていますか?	□:経営者(最高責任者)
(2)-②	総括責任者は、基本方針に則り組織横断的な管理体制を構築し、実施策を策定していますか?	□:総括責任者

No	内容	直接部門	関連部門			
			情報システム部門	総務部門	人事部門	法務・知財部門
4-2-1. 秘密指定						
(3)	重要情報を把握し、重要度に合わせて格付け区分し、取り扱い可能な内部者の範囲を定めていますか?	□				
(4)-①	重要情報の作成者は、定めた格付け区分を選択し、その選択について上司等に確認を得ていますか?	□				

図 3：内部不正チェックシート

※3　IPA「組織における内部不正防止ガイドライン」
http://www.ipa.go.jp/security/fy24/reports/insider/index.html
※4　JNSA「内部不正対策ソリューションガイド」
http://www.jnsa.org/result/2013/surv_acci/index.html

（２） 内部不正が発生する仕組み

専門家によれば、不正行為は、「不正のトライアングル」という「動機・プレッシャー」、「機会」、「正当化」の３つの要因※5が全て揃った時に発生すると言われています※6。

不正のトライアングルでは、３つの要因の低減が内部不正を防止するために有効としています。中でも能動的に組織が対策できるのは「動機・プレッシャー」と「機会」の低減です。

※5　不正のトライアングルを参考にした内部不正の３つの要因
- 「動機・プレッシャー」：プレッシャー（業務量、ノルマ等）や処遇への不満など。内部不正行為に至るきっかけとなる。
- 「機会」：技術（IT システム・ネットワーク）や物理的な環境及び組織のルールなど、内部者による不正行為の実行を可能、または容易にする環境のこと。
- 「正当化」：良心の呵責を乗り越える都合の良い解釈や他人への責任転嫁など、内部者が不正行為を自ら納得させるための自分勝手な理由付け。

※6　米国の組織犯罪研究者ドナルド･R･クレッシーによる

（３） 潜在する内部不正のリスクについて

多くの場合、内部者が不正行為を働く職場には、組織のルールに反した些細な内部不正が隠れている傾向があります※7。また、そもそもルールがない、ルールがあっても不備がある、といった場合もあります。**内部者が不正行為に至る環境を経営層が認識し、内部不正を発生させない対策と環境の整備が重要です。**そこで、2014 年に発生した内部不正の報道事例を参考に、A 社が B 社に決済処理業務を委託しているケースを想定して、内部不正行為を引き起こす要因として考えられる状況を図４に示します。

A 社：オンラインショップサービスの提供者
B 社：A 社の決済処理業務の受注社（委託先）

B 社社員は、受託した決済処理の業務システムを運用しています。

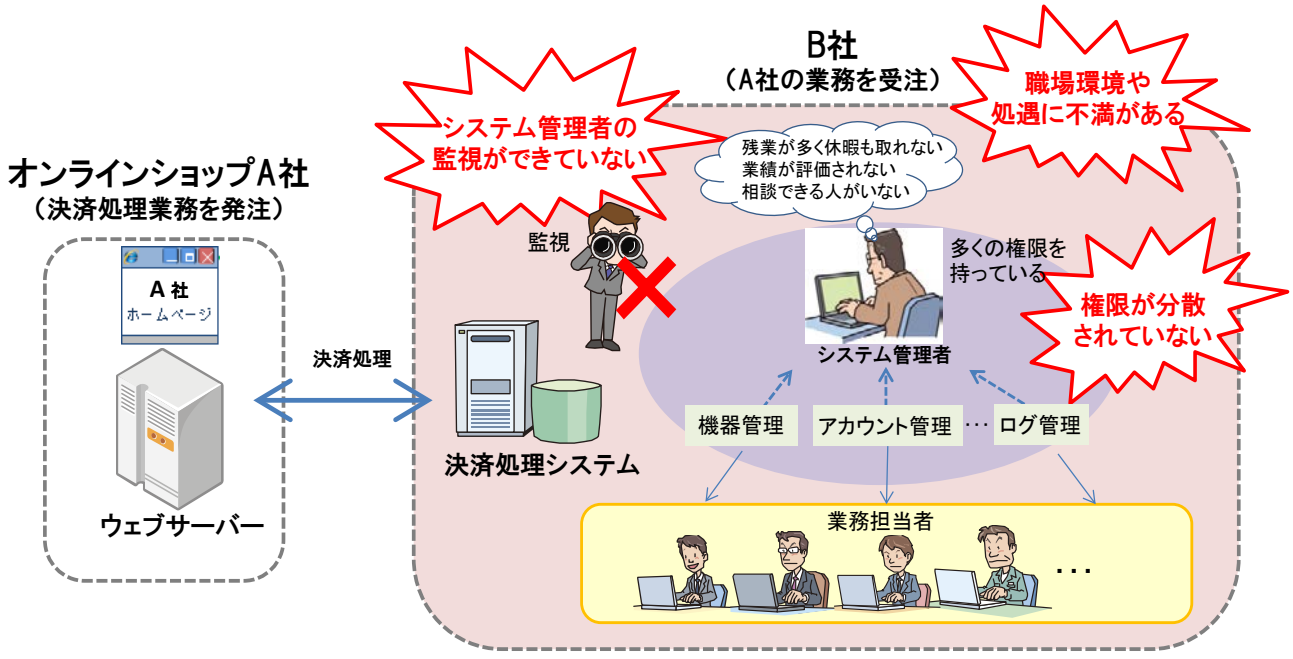

図４：委託先社員による内部不正のリスク

このケースでは、以下のような内部不正を引き起こす要因が考えらえます。

① 権限が分散されていない

B 社の特定のシステム管理者に多くの権限が集中しています。その場合、第三者の目を避け単独で顧客のクレジットカード情報などの重要情報を持ち出し、不正に使用し、さらにそれら

の操作履歴を消すことも可能になります。

② システム管理者の監視ができていない

システム管理者のアクセスや操作の履歴等のログを記録しても、その記録を監視していません。そのため、不正行為の前兆となる行為を検知することができず、発見が遅れ、被害が拡大します。

③ 職場環境が不適切、または処遇に不満がある

劣悪な労働環境では内部不正が発生する可能性が高まります。例えば、多大な業務量や長時間勤務など、B 社のシステム管理者に高負荷な状況が続くと、それがプレッシャーになり社内ルールに違反してまでも業務を遂行しようと、内部不正に至る可能性があります。また、昇進・昇格や給与等の処遇への不満、上司や同僚とのコミュニケーション不足も内部不正の要因です。

※7　ハインリッヒの法則：1 件の重大な事故・災害の背景には、29 件の軽微な事故・災害があり、さらにその背景に 300 件の重大事故につながりかねない危険な事例が存在する

（4） 内部不正防止の対策例

前述した内部不正を防止するための具体策と、IPA が 2012 年 7 月に実施した「組織内部者の不正行為によるインシデント調査」からデータを引用したポイント解説を以下に示します。

① 適切な権限管理

多くの組織は、ID やアクセス権の管理が重要であることを理解しています。以下の点に注意し、適切に権限が管理されているか再チェックしましょう。

・**特定のシステム管理者に権限が集中しないように権限を分散する**。
・**システム管理者同士が相互に監視し**、不正を行うことが困難な環境を作る。

【ポイント解説】

企業の経営者・システム管理者が考える「効果があると思う対策」は、「重要情報は特定の職員のみアクセスできるようになっている」ことが 1 位、「情報システムの管理者以外に情報システムへのアクセス管理が操作できないようになっている」が 2 位であり、アクセス管理による対策が重視されています。

しかし、昨今では、効率を求め IT 化を進めるうちに、気づいたら特定のシステム管理者が多くの権限を持っていたというケースもあるため、アクセス管理だけでなく、適切な監視ができているか再度確認しましょう。

② ログの記録と従業員への通知

「ログを残しておく」ことは、万一不正が発生しても追跡調査することを可能にし、また「ログを記録していることを従業員に知らせる」ことは、内部不正の抑止に高い効果が期待できます。重要情報へのアクセス及び操作の履歴等のログを記録するとともに、以下の点に注意しましょう。

・システム管理者のログは、**システム管理者以外の者が、定期的に確認し監視する**。
・抑止の観点から、**業務担当者にログが記録されていることを通知する**。

【ポイント解説】

社員が考える最も抑止力が高い対策は「社内システムの操作の証拠が残る（54.2%）」ですが、経営者およびシステム管理者は、21 項目中 19 位でした。

管理される側の社員と管理する側の経営者・管理者との間で有効と考える対策にギャップが

見られ、経営者が講じる対策は社員への抑止力として必ずしも効果的に機能していない可能性があります。

③ 職場環境や処遇の見直し

従業員に不正行為を踏みとどまらせる対策として、職場環境の整備が挙げられます。経営者やマネジメント層が、昇進・昇格や給与等について公平で客観的と思っていても、従業員が納得していると限りません。また、特定の従業員に常態的に負荷がかかっている状況を経営層が気づいていないかもしれません。

内部不正防止の観点から、以下を参考に職場環境について、見直しましょう。

・適正な労働環境

職場環境や労働環境を整備して、業務量や勤務時間を適正化する。また、特定の従業員の業務負荷が極端に高い状況を是正する。

・良好なコミュニケーション

相談しやすい環境を整備し、業務の支援や上司や同僚との良好なコミュニケーションがとれる職場環境づくりを推進する。

・公平な人事評価

公平で客観的な人事評価を整備し、従業員が評価内容を理解、納得できるよう、人事評価結果を説明する機会を設ける。また、適切な人員配置及び配置転換をする。

【ポイント解説】

従業員が不正行為を働く動機を高める要因だと考えるのは、組織における処遇面の不満に関する項目が上位 3 つを占めています。特に、1 位の「不当だと思う解雇通告を受けた（34.2%）」は、2 位の「給与や賞与に不満がある（23.2%）」、3 位の「社内の人事評価に不満がある（22.7%）」と比較して、割合が多くなっています。

■お問い合わせ先
IPA 技術本部 セキュリティセンター 小松／益子
Tel: 03-5978-7530　Fax: 03-5978-7546
E-mail: isec-info@ipa.go.jp