PwC's View

特集：内部監査

Vol. 4
September 2016

pwc

www.pwc.com/jp

内部不正による情報漏えいリスクに対するシステム監査

PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部
マネージャー　百歩 路子

はじめに

昨今、情報漏えいに関する事件や事故の発生により、情報漏えいリスクについて世間の注目度が高いことは周知のとおりです。このような状況を踏まえ、内部監査部門として会社が情報漏えいリスクへどのように対応しているかを把握できていますか。会社の重要な情報が悪意を持った者に不正に持ち出されないことを十分に説明できますか。

本稿では、内部監査として、企業の内部関係者による情報資産の不正持ち出しに対する評価について記載していきます。具体的には、会社の情報資産に対してどのようなリスクがあり、管理策が実施されているのかを評価し、経営層に報告して改善を促進していくために実施すべき監査アプローチを解説します。

なお、文中の意見に係る部分は筆者の私見であり、PwCあらた有限責任監査法人または所属部門の正式な見解ではないことをあらかじめお断りいたします。

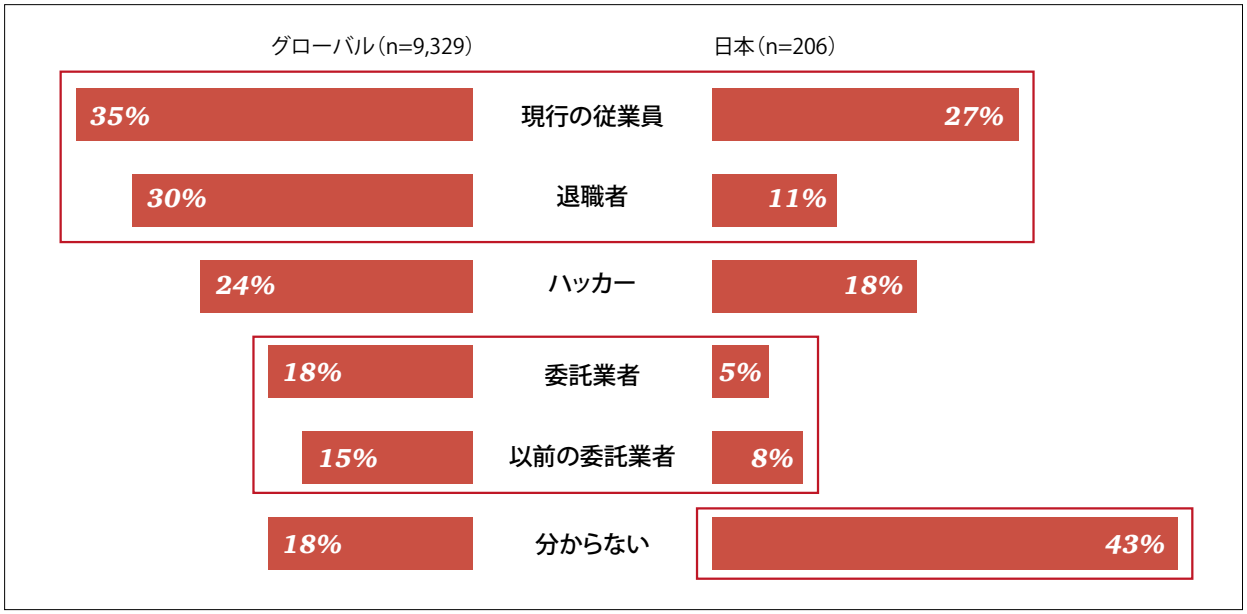
1 内部関係者による不正持ち出しの傾向

PwCが実施している「グローバル情報セキュリティ調査®2015（日本版）」によると、**図1**に示すように退職者、委託業者、以前の委託業者を含めて、情報セキュリティ上のインシデントを発生させている大多数が企業の内部関係者となっています。これは、企業が内部関係者に対して有効な管理を実施できていないと言えます。また、日本で一番多い要因が「分からない」であり、情報セキュリティ管理自体ができていないとも考えられます。

よって、企業が情報資産の管理を実践していくとともに、委託先も含めた内部関係者による不正な情報資産の持ち出しを抑止すべく、内部監査を実施するニーズが高いと言えます。

それでは、次項にて内部不正による情報漏えいリスクに関する監査アプローチについて説明します。

図1：インシデントの発生要因（グローバル情報セキュリティ調査®2015『日本版』より作成）



2 監査アプローチ

会社が保有する情報資産は多種多様であり、取り扱われる業務やシステムによって、情報の項目・形式・形態・件数も多岐にわたります。そこで、内部不正による情報漏えいリスクを想定し、情報資産の管理状況を監査するに当たっては、会社における重要な情報資産の定義と保有する情報資産の管理方法を評価する必要があります。

（1）重要な情報資産の定義

重要な情報資産として貴社ではどのような情報が定義されているかを確認する必要があります。具体的には、次の①から④の全ての項目に対して貴社では対応できているか確認します。

① 重要な情報の判断基準は明確か否か
② 当社にとって重要な情報とは、どのような情報が該当するか
③ 当社にとって重要な情報は、どこに保存されているかを漏れなく把握できているか
④ 上記①から③の内容は、社内においてコンセンサスを得ている状況か否か

上記①から④のいずれかの項目に対応できていないと想定される場合には、情報資産の定義から情報資産の分類において課題があると言えます。

よって、まずは貴社において何を重要な情報資産として管理するのかを明確にし、その定義に該当する情報の洗い出し、および保管場所を特定する必要があります。

何を重要な情報として管理すべきかは各社の業務・業態により異なるところですが、参考までに、**表1**において重要情報を識別する基礎となる情報資産の分類を整理した内容を掲載します。このような情報の分類を実施しながら、どの情報が貴社にとって重要な情報資産に該当するのかを検討することが望まれます。

また、重要情報と定義する際には、情報資産の特性を考慮して重要性を決定する必要があります。**表2**では、不正持出の観点から情報資産の特性を整理し、重要性を検討する際に一般的に活用される内容を参考までに掲載しています。

（2）情報資産の管理方法の評価

情報の不正持ち出しの管理方法を評価するには、次の三つのステップによる検討が必要です。

Step1：各情報資産に対する不正持ち出しリスクの評価

各情報資産に対する不正持ち出し、すなわち悪意者による情報を持ち出すインセンティブが存在するかを検討することが必要です。ここで言うインセンティブとは、主に情報を持ち出すことによって金銭的な利得を悪意者が享受できるか否かになることが過去の不正持ち出しの事例から一般的です。

Step2：情報を持ち出す手段に対する管理策の評価

続いて、不正に情報を持ち出すことに対する管理方法の

表1：情報資産の分類（営業秘密管理の考え方（参考1）営業秘密の類型（2013年8月経済産業省）を抜粋）

情報資産分類	情報資産分類に該当する主な情報の例
経営戦略に関する情報資産	経営計画、目標、戦略、新規事業計画、M&A計画など
顧客に関する情報資産	顧客個人情報、顧客ニーズなど
営業に関する情報資産	販売協力先情報、営業ターゲット情報、セールス・マーケティングノウハウ、仕入価格情報、仕入先情報など
技術（製造含む）に関する情報資産	共同研究情報、研究者情報、素材情報、図面情報、製造技術情報、技術ノウハウなど
管理（人事・経理など）に関する情報資産	社内システム情報（ID、パスワード）、システム構築情報、セキュリティ情報、従業者個人情報、人事評価データなど
その他の情報資産	上記以外の情報資産

表2：不正リスクの観点からの情報資産の特性

情報資産の特性	説明内容
量的	情報量が多くなればなるほど、不正持出のインセンティブが増加するもの （例）個人情報、仕入先情報　など
質的	1件のデータでも不正持出のインセンティブが想定されるもの （例）クレジットカード情報、製造技術情報　など

図2：持ち出し手段禁止のイメージ

評価では、情報への持ち出し手段に着目して監査手続きを策定します。ここで言う手段とは、次のような情報形態を外部に持ち出すための方法です。

- 電子データの場合：インターネットやメールなど
- 紙や電子記憶媒体の場合：人的な持ち出し、郵送／配送など

漏えい手段の管理方法で想定される対策としては、システム機能による制限と相互けん制等の人間による管理、またその双方の組み合わせで構築されます。**図2**では、システム機能による一般的な持ち出し手段の禁止対策を提載します。

また、管理方法については、情報を持ち出した後から検知・追跡する発見的統制ではなく、予防的統制に重きを置く必要があります。しかしながら、実際の業務を考えた場合には、情報の持ち出し手段を全て禁じることは不可能であるため、どの手段を許可しているのか会社のポリシー（規程等）で決定されていることが重要です。加えて、許可した持ち出し手段に対しては、発見的な統制が機能しているかを十分に評価していくことが肝要です。具体的には、情報の持ち出しに際して許可されていないログがないか等、すぐに検知できる体制が確保されているかを評価することになります。

Step3：残余リスクの評価

最後に、Step1で認識した不正持ち出しリスクに対して、Step2で把握した情報の持ち出し手段に対する管理策を適用した結果、想定される残余リスクの評価を行います。ここで言う残余リスクは、悪意者が不正に情報を持ち出す容易性の観点から検討します。

残余リスクが許容水準以下である場合には改善の必要性はないのですが、悪意者が単独で容易に持ち出せる場合には、残余リスクは許容水準ではないと評価するのが一般的です。

Step1からStep3をまとめた具体的な評価イメージを**図3**に掲載します。

図3：情報資産のリスクの特定および持ち出し手段の評価イメージ

情報資産（例）	リスク：競合他社への情報提供	インサイダー取引への利用	名簿業者への不正売却	反社会的勢力への不正売却	マスコミへの情報漏えい	SNSサイトへの情報公開	インターネットへの不正情報公開	漏えい手段に対する予防的管理策：紙	電子記憶媒体	スマートフォン	メール	インターネット	残余リスク
新製品の情報	✓	✓			✓	✓	✓	◎					
仕入価格	✓					✓	✓	×					
M＆A情報	✓	✓		✓	✓	✓	✓	◎					
顧客情報	✓		✓	✓				◎					

情報にアクセス可能な全ての人間に対するコントロールの有効性を検討する

想定される残余リスク

3 評価対象範囲を検討する際の留意点

「1.内部関係者による不正持ち出しの傾向」で言及したように、委託業者、以前の委託業者が悪意者として想定されるため、外部委託先も含めて評価する必要があります。そこで、外部委託先に対して情報漏えいリスクをテーマとした内部監査を実施するには、「2.監査アプローチ」で記載した内容に加えて、評価範囲および内部監査の実施を担保するために次の三つのステップによる確認が必要です。

Step1：自社内の重要な情報資産を外部委託先に預託しているか

業務を外部業者に委託する際に、重要な情報資産を預託している場合には当該委託先が監査対象の候補として想定されます。

Step2：外部委託業務の1次請け、2次請け等の関係を把握しているか

Step1で該当した委託業務のサービス提供体制を確認します。特に自社の重要な情報資産はどの委託先まで展開されているのかを把握することが必要です。

Step3：監査権は担保されているか

Step2で把握した自社の重要な情報資産を活用して業務を実施している委託先に対して、監査権が担保されていなければ、そもそも内部監査を実施することができません。そのため監査権が確保されていない場合には、委託元部門に対してまずは監査権の確保を促す必要があります。

一方で、私たちが支援しているケースにおいては委託先が協力的である場合もあり、必ずしも監査権が契約上明記されていなくとも、監査に協力してもらえるケースもあります。よって、まずは内部監査を実施したい旨を打診することも重要です。

このように、外部委託先を評価する際には評価範囲の網羅的な理解、および監査の実施の担保というプロセスが追加で必要となる点に留意が必要です。

4 内部監査結果の有効活用

情報セキュリティに対する対策は、IT設備の導入等が必要となるケースもあるため、導入までに中長期間を要することも想定されます。しかしながら、検出された事項が会社にとって早急に対応した方がよいと考えられる事項に関しては、ベストプラクティスを前提とした発見事項に基づき改善を促すだけでなく、ベタープラクティスも改善案として提示することにより残余リスクを確実に低減していくことが重要です。このような改善を促すことで、主として対策実施者となり得るIT部門や総務部門等も納得感ある監査として受け入れることができると想定されます。

繰り返しになりますが、情報セキュリティに対する投資は成果としてのリターンが明確に認識できないものです。昨年末に公開された「サイバーセキュリティ経営ガイドライン」（経済産業省）においてもセキュリティ投資に対するリターンを求めない旨が言及されており、費用対効果の観点から改善提案を立案することは重要であるものの、投資対効果の観点から改善案をいたずらに制限するのは避けるべきであると言えます。

5 おわりに

会社の情報資産を持ち出されないための情報漏えいリスクに関する監査アプローチとリスク評価について述べてきました。監査結果で浮き彫りになった不十分な管理状況について、経営層が許容可能なリスク水準と現場が対応可能な管理対策を踏まえて、内部監査が現場と経営層とコミュニケーションを密に取りながら改善を進めていくことが望まれます。

一方で、内部不正による情報漏えいを鑑みると、情報に触れる機会をなくすことが不正根絶への近道と言われています。情報を不必要に「持たない、見せない、作らない」をモットーに監査を通じて、必要以上に情報を保有していたり複製を作成していたりするケースが見受けられた場合には、啓蒙活動の一環として気付きに取り上げてみてはいかがでしょうか。

本稿が、貴社における情報資産の管理状況を監査する際の一助になりましたら幸いです。

百歩 路子（ひゃくぶ みちこ）
PwCあらた有限責任監査法人
システム・プロセス・アシュアランス部 マネージャー
PwCに入所後、主として金融機関の監査業務を担当。財務報告に係る内部統制対応の評価支援や内部監査におけるシステム監査支援、システム監査に関するアドバイザリー業務を実施。近年ではシステムリスク管理態勢の構築支援、システム障害管理態勢の有効性評価をはじめ、顧客情報を取り扱う外部委託先に対する情報セキュリティ評価、機密情報を扱う業務・システムに対する情報セキュリティ監査、サイバーセキュリティ対応態勢の評価等に多数従事。
メールアドレス：michiko.hyakubu@jp.pwc.com

PwCあらた有限責任監査法人
〒104-0061
東京都中央区銀座 8-21-1　住友不動産汐留浜離宮ビル
Tel：03-3546-8450　Fax：03-3546-8451