損保ジャパン日本興亜RMレポート| 121

企業内部の不正行為による情報流出リスク

井口　洋輔　Yosuke Iguchi
リスクコンサルティング事業本部 ERM 部
主任コンサルタント

はじめに

ウィルスやハッキングによるサイバー攻撃、技術情報の不正な持ち出し等、情報セキュリティ事故が連日のように報道され、さらに「企業内のルール違反」や「うっかりミス」を含めると、情報セキュリティ事故が後を絶たない状況にある。情報流出は、企業・組織（以下、「企業」）にとって顧客・株主などのステークホルダー（利害関係者）からの信頼喪失や多額のお見舞い金・損害賠償金などの経済的損失につながる。

近年発生している情報セキュリティ事故のうち、企業への信頼喪失や経済的損失が大きい事案の発生要因を分析すると、「外部からの攻撃」と「内部の不正行為」の大きく 2 つに分類することができる。外部からの攻撃は一般的にサイバー攻撃とも言われ、ウェブサイトの改ざん、DDoS（Distributed Denial of Service attack）攻撃[1]、標的型攻撃メール[2]等が当てはまる。一方、内部の不正行為としては、退職者による技術情報等の重要情報[3]の流出や従業員による顧客情報の不正な売却等が挙げられる。特に内部の不正行為による重要情報流出の被害は年々深刻化してきており、経営の根幹を脅かすリスクの一つとして注目が高まっている。

そこで、本稿では、企業内部の不正行為による重要情報の流出実態を示すとともに、それらを踏まえて情報セキュリティの観点から検討すべき有効な対策のポイントについて解説する。

1. 重要情報流出の実態

2014 年 7 月 17 日に、大手通信教育会社の顧客情報を販売目的で不正に取得して社外に漏洩させたとして、システム開発・運用を行っているグループ会社の業務委託先の元従業員であったシステムエンジニアが不正競争防止法違反容疑で逮捕されたことは記憶に新しいところである。同事案以外にも正当なアクセス権限を持つ者やアクセス権限を持っていた退職者等の内部者による不正行為の事案が相次いで報道されている（表 1）。

[1] 多数のパソコンから一斉に大量のデータを特定の宛先に送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃
[2] 情報窃取を目的として特定の宛先に送られるウィルスメール
[3] 技術、ノウハウ、図面、デザイン、仕様書、作業手順書等といった技術的な情報のみならず、経営計画、顧客・取引先情報等の所有者にとって資産性又は価値を有する情報

表 1　内部者の不正行為によって重要情報が流出した主な事案[4]

○元技術者による研究データの流出
日本の大手電機メーカーの元技術者が、米国の半導体メーカーの技術者として日本メーカーの工場に勤務していた時に会社のサーバにアクセスし、営業秘密であるフラッシュメモリーの実験データ等を不正に所得して転職先である韓国の大手半導体メーカーに持ち込んだ。その後、元技術者は不正競争防止法違反（営業秘密開示）で逮捕された。
○元従業員による発売前の新型車情報の流出
大手自動車メーカーの元従業員が、退職する直前に、会社のサーバにアクセスして発売前の新型車情報等の営業秘密を不正に取得し、新たな就職先に持ち込んだ。その後、元従業員は不正競争防止法違反（営業秘密領得）の疑いで逮捕された。
○委託会社の元従業員によるカード情報の不正持ち出し
銀行の ATM の保守管理業務の委託先会社の元従業員が、ATM の取引データから顧客のカード情報を不正に取得した。その後、不正に取得した顧客情報を基に偽造キャッシュカードを作成・所持していた容疑で逮捕された。
○元従業員による製造技術の不正流出
日本の大手鉄鋼会社が、韓国の鉄鋼最大手会社らに対し、鋼板の製造技術を日本の大手鉄鋼会社の元従業員経由で営業秘密を不正に取得・使用したとして、約 1,000 億円の損害賠償および製造販売等の差止めを求めて、東京地方裁判所に訴訟を提訴した。
○元従業員から技術情報流出
大手工作機械会社の元従業員が、不正の利益を得る目的で、社用パソコンから会社のサーバに接続し、営業秘密として扱われていた工作機械の設計情報等のファイル 6 件を取得した。その後、私物のハードディスクに複製して持ち出したとして、不正競争防止法違反（営業秘密の不正取得）の刑事責任が問われた。
○証券会社のシステム担当部長による顧客データの持ち出し･売却
証券会社のシステム担当であった元部長代理が、会社のデータベースに不正にアクセスして約 148 万人分の顧客データを持ち出し、そのうち約 5 万人分の顧客データを名簿業者に売却した。その後、元部長代理は不正アクセス禁止法違反と窃盗の容疑で逮捕された。

また、経済産業省の「営業秘密の管理実態に関するアンケート調査」[5]によると、営業秘密の漏洩を経験した企業の漏洩経路としては「中途退職者（正規社員）による漏洩」の割合が最も高く 50.3%となっている。次いで、「現職従業員等のミスによる漏洩（26.9%）」、「金銭目的等の動機をもった現職従業員等による漏洩（10.9%）」となっており、重要情報の流出においては内部者の関与が多くを占めていることが見てとれる（図 1）。

[4] 経済産業省「技術情報等の適正な管理の在り方に関する研究会 報告書」および新聞報道をもとに当社作成
[5] 経済産業省「営業秘密の管理実態に関するアンケート調査」調査結果（確報版）

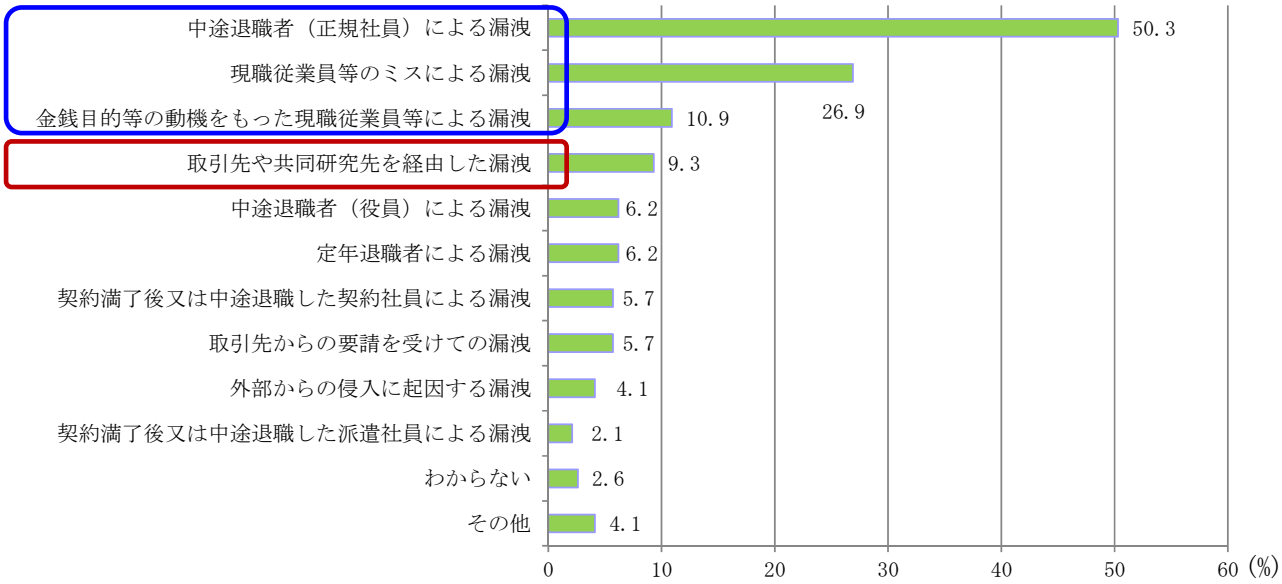

図 1　重要情報の主な流出経路[6]

さらに、取引先の情報管理体制の不備による内部不正から重要情報が流出してしまうケースや、提携先が意図的に秘密保持契約に違反して重要情報を流出するケース等が注意すべき流出経路として挙げられる。さらに、業界再編等によって、買収や合併、事業の切り離し、新会社設立等の動きの中で、当事者となる企業間の情報管理レベルの違いや退職者の増加により、重要情報が流出してしまう可能性があることにも留意いただきたい。

2. 企業が実施すべき内部不正対策

内部者による不正行為を防止するための対策を検討する際には、報道や判例で公開された事案以外にも裁判に至らない事案やヒヤリ・ハットに関する事案について幅広く情報を収集することが有用となる。近年、個人情報の漏洩は公表[7]されることが多くなった[8]。しかし、重要情報に係る内部不正の場合には信頼や評判が損なわれるといった負の影響を懸念し、企業内部や当事者間で処理されてしまう傾向にあり、その実態を把握しにくいのが実情である。そこで、不正行為者が不正行為を働く動機や背景等を踏まえた上でそれらを排除することが、内部不正への対策を検討する際に有効であることから、その一部を紹介する。

2.1. 内部不正を防止するために取り組まれている対策の現状

独立行政法人情報処理推進機構が実施した「企業内部者の不正行為によるインシデント調査－調査報告書－」[9]によると、管理される側（従業員）と管理する側（経営者・システム管理者）では内部不正に効果的であると考える対策について、認識に大きな違いが見られる。「内部不正行為に効果が期待できる対策」という設問に対して、従業員の回答は「社内システムの操作の証拠が残る（54.2%）」、「顧客情報などの重要な情報にアクセスした人が監視される（37.5%）」が上位を占めている（図 2）。一方、同じ質問に対する経営者やシステム管理者の回答は「開発物や顧客情

[6] 「営業秘密の管理実態に関するアンケート調査」（経済産業省）に当社にて一部追記
[7] 政府「個人情報の保護に関する基本方針」（6 個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項）平成 16 年 4 月 2 日閣議決定、平成 21 年 9 月 1 日一部変更
[8] NPO 日本ネットワークセキュリティ協会「情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」
[9] 独立行政法人情報処理推進機構「企業内部者の不正行為によるインシデント調査－調査報告書－」

報などの重要情報は特定の職員のみアクセスできる(20.9%)」、「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(12.7%)」が上位を占めている(図 3)。

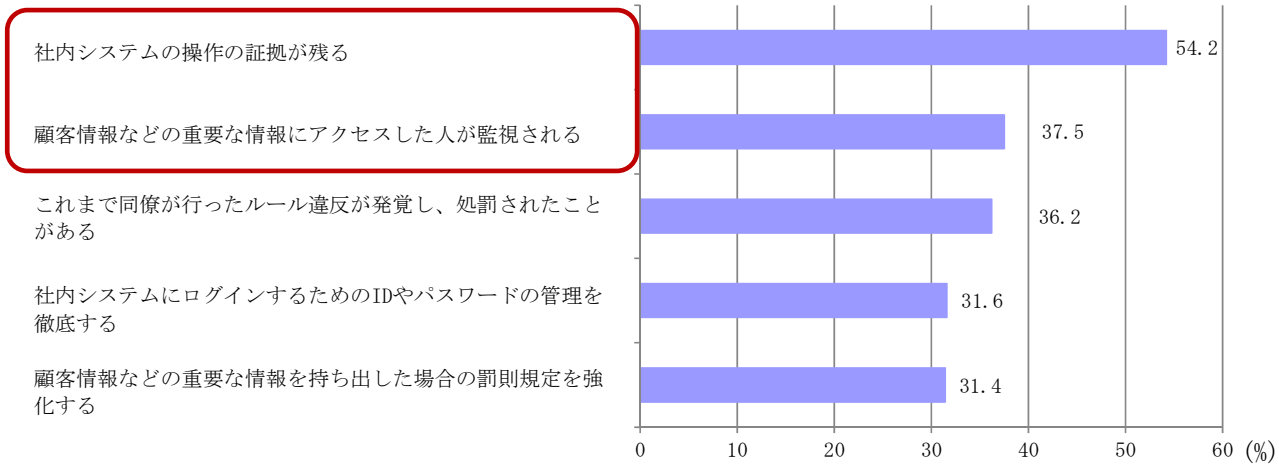

図 2　従業員が内部不正行為に対して効果的であると考える対策[10]

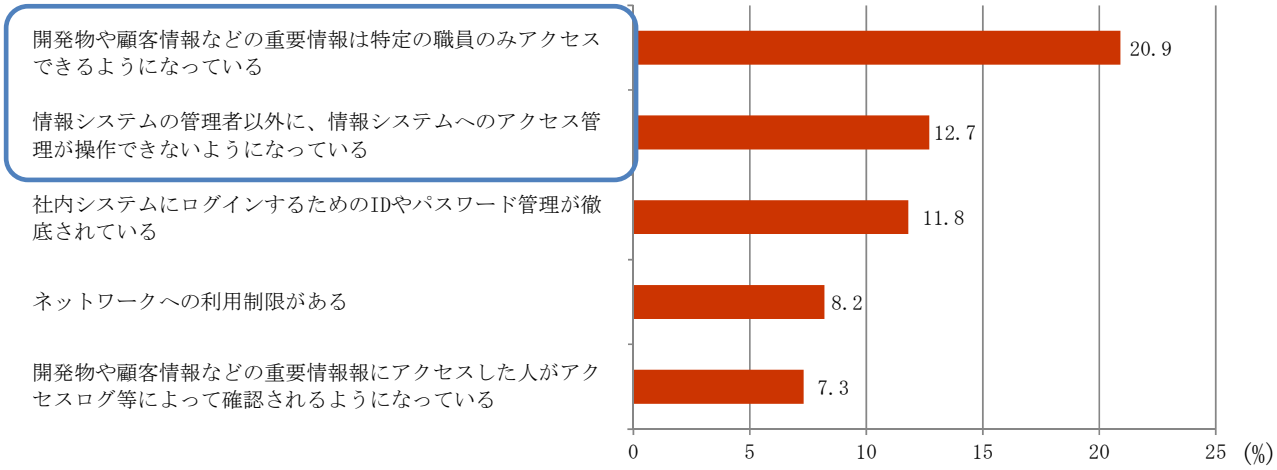

図 3　経営者・システム管理者が内部不正行為に対して効果的であると考える対策[11]

上記の調査結果より、従業員は「証拠を発見される（内部不正を行う気にさせない、動機・プレッシャーを低める）対策」に効果があると感じているのに対し、経営者・システム管理者は「アクセスさせない（不正の機会を作らない）対策」が効果的であると考え、内部不正対策への認識にギャップがあることが分かる。すなわち、アクセス権の有無に関わらず優先的に考慮しなければならないのは、“組織としての証拠確保能力を高め、かつ問題の発生を抑止するためのモニタリング体制をいかに整備していくか”であることが調査結果より見てとれる。まずは、流出した場合の影響とコストを判断しつつ、影響が大きい重要情報に対して、前述のギャップを解消する必要性について検討することをお勧めする。

2.2. 効果的に内部不正対策を実施するためのポイント

企業が情報管理体制を整備する際には、書類・媒体の施錠保管や保管場所への入退室制限（物理的管理）、ウィルス対策ソフトの導入やアクセスログの取得・チェック（技術的管理）、従業員への教育・研修や取引先

[10] 独立行政法人情報処理推進機構「企業内部者の不正行為によるインシデント調査－調査報告書－」に当社にて一部追記
[11] 独立行政法人情報処理推進機構「企業内部者の不正行為によるインシデント調査－調査報告書－」に当社にて一部追記

との秘密保持契約の締結（人的管理）等を検討することになる。表 2 は、効果的に内部不正対策を整備するための観点および必要な対策を情報セキュリティの観点から網羅的に示したものである。

表 2　内部不正対策を検討する際の観点および対策[12]

観点		対策
1.基本方針		経営者の責任の明確化
		総括責任者の任命と組織同断的な体制構築
2.資産管理	秘密指定	情報の格付け
		格付け区分の適用とラベル付け
	アクセス権指定	情報システムにおける利用者のアクセス管理
		システム管理者の権限管理
		情報システムにおける利用者の識別と認証
3.物理的管理		物理的な保護と入退管理策
		情報機器及び記録媒体の資産管理及び物理的な保護
		情報機器及び記録媒体の持出管理及び監視
		個人の情報機器及び記録媒体の業務利用及び持込の制限
4.技術・運用管理		ネットワーク利用のための安全管理
		重要情報の受渡し保護
		情報機器や記録媒体の持ち出しの保護
		組織外部での業務における重要情報の保護
		第三者が提供するサービス利用の確認（クラウドコンピューティングを含む）
5.証拠確保		情報システムにおけるログ・証跡の記録と保存
		システム管理者のログ・証跡の確認
6.人的管理		教育による内部不正対策の周知徹底
		雇用終了の際の人事手続き
		雇用終了及び契約終了による情報資産等の返却
7.コンプライアンス		法的手続きの整備
		誓約書の要請
8.職場環境		公正な人事評価の整備
		適正な労働環境及びコミュニケーションの推進
		職環境におけるマネジメント
9.事後対策		事後対策に求められる体制の整備
		処罰等の検討及び再発防止
10.組織の管理		内部不正に関する通報制度の整備
		内部不正防止の観点を含んだ確認の実施

[12] 独立行政法人情報処理推進機構「組織における内部不正防止ガイドライン」

重要情報の正当なアクセス権限を持つ管理者やアクセス権限を持っていた退職者による不正の実行は本人の気持ち次第であり、いつ発生してもおかしくないリスクである。そのため、予防や抑止の観点から対策を実施するのみでは十分と言えず、内部不正の発生を前提とした事後対応力の整備が求められる。万が一、内部不正によるインシデントが発生した場合には、まず被害拡大の防止や原因の特定、影響範囲の特定等が求められ、その後処罰等の検討や再発防止策を実施する流れになる。具体的には、不正行為を行った PC 等の保全、各種ログの保全等を行い、デジタルフォレンジック[13]等による不正操作の解析を行うことができるようにする必要がある。また、必要に応じて、警察、弁護士、内部監査者、調査専門業者、保険会社等と連携して対応し、さらに監督官庁への報告義務がある場合は速やかに報告できる体制を用意しておくことも重要になる。これらの体制の充実は、2.1 で示したギャップの解消に繋がるだけでなく、犯行に及ぼうとする者に犯人として特定されるリスクを具体的に認識させる副次的な効果もある。

以上のことから、内部不正が発生した場合に取るべき事後対応および法的手続きに関連する「2.資産管理（秘密指定、アクセス権設定）」、「5.証拠確保」、「6.人的管理」、「7.コンプライアンス」については、最低限実施すべきである。特に「証拠確保」においては情報システムにおけるログ・証跡が保存されていないと、有時の事後対応において、内部不正の原因の特定および内部不正者の追跡、影響範囲等の調査に大きな影響を及ぼすことになる。最近では e ディスカバリー（電子証拠開示）やカルテル調査等の場面において訴訟に耐えうる証拠保全の必要性が高まっていることからも「証拠確保」について実施を検討いただきたい。このような状況の中、検討すべき対策は他にもあるが、まずは表 3 の対策内容を踏まえて自社の証拠確保能力が整備できているか確認することをお勧めする。

[13] インシデント・レスポンスや法的紛争・訴訟に対し、デジタル機器上に残る記録の証拠保全および調査・分析を行うとともに、デジタル機器上に残る記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術

表 3　情報セキュリティの観点から証拠確保能力を高める対策例[14]

□重要情報を重要度に合わせて格付け区分し、取扱い可能者の範囲を定めている
□重要情報を含む電子文書には、機密であることを示す言語・文字・マーク等の表示をしている
□情報システムの利用者 ID およびアクセス権の登録・変更・削除等の手順を定めて運用している
□異動又は退職により不要となった利用者 ID およびアクセス権は直ちに削除している
□重要情報へのアクセス履歴および利用者の操作履歴等のログ・証跡を定めた期間に従って安全に保護している
□抑止の観点からログが記録されていることを従業員等に通知している
□USB メモリ、外付 HDD、スマートフォン等の外部機器と PC の接続を制限している
□利用している OS、アプリケーション、ミドルウェアの情報を確認し、脆弱性情報やパッチ情報を管理している（あるいは直ぐに確認できる状態になっている）
□データ・HDD の暗号化を実施している場合、暗号化を復号する情報（キーコード等）が直ぐに確認できる状態になっている
□サーバ、ネットワーク機器等の特権アカウントの種類・付与対象者・付与人数を管理している
□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している
□共有アカウントを廃止し、システム管理者（利用者）ごとに利用者 ID を割り当てている
□システム管理者が 1 人の場合、操作履歴をシステム管理者以外の者が定期的に確認している
□会社が貸与している退職予定者の PC、携帯電話・スマートフォン等の機器を回収・保管し、退職前や退職後にも必要に応じて調査可能な状態にしている
□内部不正の影響範囲を特定するために、事象の具体的状況を把握するとともに、被害の最小化策や影響の拡大防止策を実施し、必要に応じて組織内外の関係者との連携体制を確保している

さらに、実施している対策の実効性を確保するためには、重要情報に対する従業員の意識を養成する「Know How」や「Know Why（なぜそれを実践しなければならないか）」を繰り返し周知徹底させていくことが重要になってくる。また、金銭目的や転職を有利に進める等の動機をもって退職者が重要情報を流出していることを鑑みると、退職時に秘密保持義務や競業避止を課す誓約書等の提出だけでなく、会社が貸与している退職予定者の PC、携帯電話・スマートフォン等の機器を回収・保管し、退職後はもとより退職前にも必要に応じて調査可能な状態にしておくことも有効である。

おわりに

近年増大する重要情報流出事案を紐解いて見ると、正当なアクセス権限を持つ管理者やアクセス権限を持っていた退職者等の内部者を通じた流出事案が多く見られる。特に、正当なアクセス権限のない者には、漫然と対策を実施するだけではどうしても限界が出てきてしまう。表 2 や表 3 で示した対策に加えて、内部不正が発生する環境要因や不正行為者の心理的な要因等を踏まえつつ、自社の実態に見合った形で態勢を整備・見直していくことが望まれる。また、見直しに向けては、性善説・性悪説・性弱説などの考え方で対策の必要性が語られることもあるが、これらの諸説の観点を根拠に企業が対策を検討する際には、企業が従業

[14] 当社作成

員を「信じるか」「信じないか」という企業の姿勢に対する単純化された議論にもなり易いのでご留意いただきたい。あくまでも内部不正への対策の見直しにおいては、顧客や株主等の要請や期待および従業員の理解などに対する説明責任を考慮し、自社のリスクに応じた合理的な根拠をもって対策を見直されることをお勧めする。なお、当社では本稿で述べた観点から態勢を整備していくための「予防策」や「事後対応」のコンサルティングを行っているので、ぜひご活用いただきたい。

参考文献

経済産業省「技術情報等の適正な管理の在り方に関する研究会 報告書」
経済産業省「営業秘密の管理実態に関するアンケート調査」調査結果（確報版）
NPO 日本ネットワークセキュリティ協会「情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」
独立行政法人情報処理推進機構「企業内部者の不正行為によるインシデント調査－調査報告書－」
独立行政法人情報処理推進機構「組織における内部不正防止ガイドライン」

執筆者紹介

井口　洋輔　Yosuke Iguchi

リスクコンサルティング事業本部 ERM 部
主任コンサルタント
専門は情報セキュリティ、個人情報保護

損保ジャパン日本興亜リスクマネジメントについて

損保ジャパン日本興亜リスクマネジメント株式会社は、損保ジャパン日本興亜グループのリスクコンサルティング会社です。全社的リスクマネジメント（ERM）、事業継続（BCM・BCP）、火災・爆発事故、自然災害、CSR・環境、セキュリティ、製造物責任（PL）、労働災害、医療・介護安全および自動車事故防止などに関するコンサルティング・サービスを提供しています。
詳しくは、損保ジャパン日本興亜リスクマネジメントのウェブサイト（http://www.sjnk-rm.co.jp/）をご覧ください。

本レポートに関するお問い合わせ先

損保ジャパン日本興亜リスクマネジメント株式会社
リスクコンサルティング事業本部 ERM 部
〒160-0023 東京都新宿区西新宿 1-24-1 エステック情報ビル
TEL：03-3349-4226（直通）

