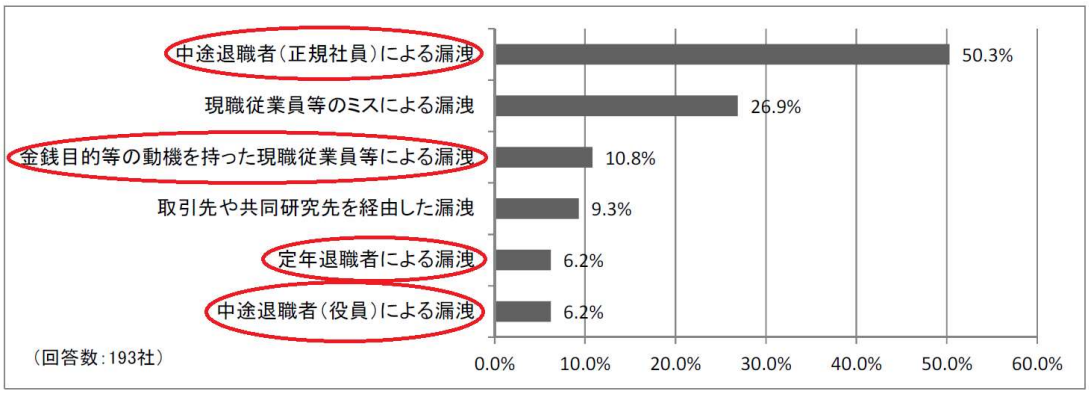
営業秘密の情報漏洩は会社崩壊を招く／事例・予防策・事後対応を解説

2018/02/06

2015年秋、ある退職社員が前職の会社からUSBメモリーにコピーした顧客情報を、転職先の営業活動に利用したという不正競争防止法違反の疑いで逮捕されました。 社内に精通する退職社員による不正は被害が大きくなる傾向があります。この事件も、転職元である被害を受けた会社が警察に告訴するほどの状況でした。**営業秘密の漏えいに関しては、62.7%が退職社員・役員・定年退職者によるもの**、これは退職社員による不正の重大性を示しています。また現職社員でも金銭目的のための不正流出に手を貸していることを考えれば、**会社内からの営業秘密情報漏えいは実に73.5%（※）**にもなります。



※経済産業省「人材を通じた技術流出に関する調査研究報告書」(2013年3月)

本稿では、情報漏えいに対する基本的な法的対応についての説明とともに退職前、退職後にできる具体的な対策と事例についても説明します。

目次

1. 退職予定者が使用する主な4つのツール　事例と予防・対策

※当社調べ(発生率：%)

1-1. 会社メール（13%）

＜事例＞

ある退職予定者が、顧客情報や新規事業の資料等を私的に利用するため会社メールで自らの私用メールアドレスに送信し、送信後メール履歴を削除した。退職後独立し、この顧客情報等を利用して顧客を開拓していたことが判明。この元社員に対し損害賠償を求める訴訟を起こすこととなった。

＜予防・対策＞

メールの履歴は削除されても復元することが出来ます。メールを使った情報漏えいの証拠は、削除されたメールを復元することで発見出来る可能性があります。

復元方法は 5.まとめ をご覧ください。

1-2. フリーメールによる漏えい（33%）

＜事例＞

ある退職予定者は、私用のフリーメール（GmailやヤフーメールやYahoo!メール等）をインターネットブラウザで立ち上げ、仕入先／原材料リストや価格表／原価表等の秘密データを添付して転職先企業に送信して情報を漏洩した疑い。

＜予防・対策＞

ログ監視ツールを導入していてもフリーメールでの本文や添付ファイルは確認できない場合があります。ですから、制御ソフトでインターネットのフリーメールサイトにアクセス出来ないようにすることをお奨めします。また、会社メール以外のフリーメールのアカウントを登録していないか、抜き打ち監査するとともに、会社指定以外のメールソフトは、インストール禁止、実行禁止にすることでリスクを低減できます。

1-3. クラウドストレージによる漏えい（23%）

＜事例＞

ある退職予定者は、クラウドストレージ（OneDriveやDropbox等）を利用して自宅のPCと同期するフォルダを設定し、そのフォルダに会社メールのバックアップや社外秘の顧客リスト等を保存。自動的に自宅PCに送り情報を漏洩した。退職後、競合他社へ転職し、顧客情報等を流用した疑いが浮上する。転職先での顧客情報利用の有無については明確にできず、訴訟には至っていない。

＜予防・対策＞

漏洩した情報によって被った損害については、明確に出来ない場合も多いです。まずは、漏洩を未然に防ぐ環境を整えることが重要です。クラウドストレージについてはソフトウェアとWebサービスの両方を制限する必要があります。ソフトウェアはインストール禁止にし、Webサービスはインターネットのアクセスを制限することで対策できます。

1-4. SNSや掲示板への漏えい（8%）

＜事例＞

ある退職予定者は、未発表の新商品の名前や仕様を匿名のSNSや掲示板へ投稿して情報を漏洩した。

＜予防・対策＞

会社PCからのSNSや掲示板へのアクセスを禁止するとともに、Webのモニタリングを実施することも早期発見の有効な手段となります。

2. コストを最小限にすぐにできる情報漏えい予防策チェック一覧

2-1. 予防策　5カテゴリ25項目

これまで事例や対策を見てきましたが、そもそも犯罪防止という観点からそこまで費用をかけずに予防策を実施する方法に関してもお伝えします。**特に赤い〇印をつけた箇所をチェック**してみてください。以下の表は社内犯罪を防ぐという観点からどのような環境や社員の心理に訴えかけていくかを検討した内容となりますので少し極端な内容も含まれるためです。すでに実施されていることが多く目に付くかもしれませんが、すぐにもできる防止策の取りこぼしを防ぐ意味でもチェックしてみてください。

犯行を難しくする	捕まるリスクを高める	犯行の見返りを減らす	犯行の挑発を減らす	犯罪を容認する言い訳を許さない
1.犯行対象を防御的に強化する ・スクリーンロックの設定 ・アクセス制御の設定 ・退職者の ID 削除/確認者設置 ・パスワードポリシーの設定 ・PC の物理チェーンロック、固定具 ・盗用防止スクリーン	6.監視者を増やす ・複数人での作業環境の設定 ・防犯ベルの設置 ・特権階級の分散化/管理者の増員 ・個人情報売買の監視 ・アクセスログの監視	11.標的を隠す ・電子ファイルのアクセス権限の設定 ・PC/USB メモリの保管場所設定	16.欲求不満やストレスを減らす ・職場での円滑なコミュニケーションの推進 ・上司や同僚に頻繁に相談できる環境整備 ・適切な人事・作業管理(業務量の軽減)	21.規則を決める ・情報セキュリティポリシーの策定 ・個人情報管理策の作成 ・就業規則 ・障害対策等の手順の明確化 ・管理/運用策の策定 ・雇用契約
2.施設への出入を制限する ・ID カード(身分証明)の確認 ・電子カードアクセス ・手荷物検査	7.自然監視を補佐する ・守りやすい空間の設計(外部から見えるガラス面積の拡大) ・オフィスのフリースペース化 ・投書箱による密告者をサポートする	12.対象を排除する ・電子ファイルのアクセス権限の設定 ・PC の持込許可制度 ・業務上で必要な閲覧項目を絞る ・紙の廃棄/溶解処理	17.対立を避ける ・情報セキュリティの管理部門を設置し、上司との対立を避ける ・適切な人事・作業管理(業務量の軽減)	22.指示を掲示する ・情報セキュリティポリシーの掲示 ・個人情報管理策の掲示 ・就業規則の掲示 ・目的外利用の禁止の掲示 ・不正事例の掲示(匿名)
3.出口で検査をする ・ID カード(身分証明)の確認 ・手荷物検査 ・メールやネットの監視	8.匿名性を減らす ・ID カード、社員バッチの携帯 ・ID による管理 ・持ち出し台帳による管理	13.所有物を特定する ・PC/USB メモリに登録番号シールをつける ・電子ファイル/紙ファイルに管理番号をつける ・複写台帳管理	18.感情の高ぶりを抑える ・パワハラの禁止 ・人種的中傷の禁止 ・適切な人事・作業管理(業務量の軽減)	23.良心に警告する ・持ち出し厳禁であることを掲示 ・管理レベルを表示/印字 ・不正競争防止法などの研修・教育 ・ルール厳守への自己サイン
4.犯罪者をそらす ・通路/出入り口の閉鎖 ・物理レベルに応じた入退制限 ・金属探知器	9.現場管理者の利用 ・CCTV(監視カメラ)の設置 ・機密情報へのアクセスは複数人による作業制限	14.市場を阻止する ・不正競争防止法 ・不正監査/不正検査 ・個人情報売買の禁止/監視	19.仲間からの圧力を緩和する ・適切な人事・作業管理(業務量の軽減)	24.遵守を補佐する ・利用 PC/USB メモリの登録管理/貸出規則を簡単にする ・施錠保管キャビネットの設置 ・シュレッダーの設置 ・相談窓口の整備
5.道具や対抗手段を制御する ・非登録の PC/CD/USB メモリの持込/持出/書出し禁止 ・携帯電話の持ち込み禁止 ・メールやネットの利用制限・禁止(フィルタリング等)	10.フォーマルな監視体制を強化する ・侵入警報装置 ・警備員	15.利益を否定する ・重要情報の暗号化 ・重要情報にノイズや電子透かし各種ウォーターマークを注入	20.模倣犯を阻止する ・インシデントの手口の公開を慎重にする ・インシデントの証跡を残さない	25.薬物・アルコールを規制する ・職場での飲酒禁止/検査 ・アルコールなしの行事

図 3 状況的犯罪予防(ITセキュリティ対策版)

(出典)5 カテゴリ 25 分類は、(財)社会安全研究財団:「環境犯罪学と犯罪分析」P191 を参考とし、セキュリティ対策の例を作成

2-2. 最低限のサイバーセキュリティ4つ

標的型攻撃メールや不正アクセスなどが怖いと聞くけれど、何から対策を始めていいのか分からない･･･、ここでは「事業活動において、請求書や納品書のやり取りなどにメールを利用しているけれど、セキュリティ対策まではまだ手が付けられていない」というような事業者の方が、“まず”何から始めればよいか、という観点で、以下４つをを最低限のサイバーセキュリティ対策として経済産業書の『秘密情報の保護ハンドブック（平成28年2月）』からご紹介いたします。

① ソフトウェアは常に最新版にアップデートする

② ウィルス対策ソフトを導入する

③ ファイヤオールを設定する

そして最後に、“いざという時のために”

④ システムのログ（履歴・記録）の設定を確認する

・サーバーや機器のシステム時刻を合わせる

➡ 時刻が合っていないと、いざというときにいつ何があったか分からないため

・ログが記録・保存できる期間に注意する

➡ どのくらいの期間や容量を記録・保存できるのか確認し、適切にチェックされるような体制をつくる

3. ＜発覚＞退職後の情報漏えいに対する法的対応について

不正競争防止法上、3つの要件が揃ったものは「営業秘密」として特別に保護されています。

【営業秘密の3要件】
・情報の有用性
・情報が一般に知られていないこと

・情報が秘密として管理されていること

営業秘密を漏洩した退職社員に対しては、話し合いによる解決（示談）のほか、以下のような法的対応の可能性があります。

3-1. 民事訴訟提起

退職社員が営業秘密を持ち出して独立・転職先で利用しているような場合、民法上の不法行為や債務不履行による損害賠償請求、不当利得返還請求、 謝罪広告等の信頼回復措置請求のほか、不正競争防止法で営業秘密利用 の差し止めや廃棄、損害賠償請求をすることが考えられます。

3-2. 刑事告訴・告発

退職社員の営業秘密持ち出しや利用の態様によっては、被害を受けた会社が告訴・告発することで警察による捜査が行われて裁判で有罪となれば、不正競争防止法21条で最大10年以下の懲役・1000万円以下の罰金に処されます。 退職社員が転職した先の会社が共犯と認められれば、同法22条により転職先の会社に対して3億円以下の罰金が科せられます。

4. ＜発覚＞法的対応をとるためのデジタル証拠収集方法

4-1. ＜予防・準備＞　PC操作ログ監視ツール

営業秘密であるというために、IDパスワード管理等で誰でもアクセスできる状況であってはならないのは当然ですが、退職社員に対する法的措置を取るにあたっては 以下のようなデジタル証拠を押さえておく必要があります。

① 営業秘密へのアクセス履歴

② 営業秘密をUSBメモリ等の持ち出し可能な記憶媒体にコピーした履歴

③ 営業秘密を印刷した履歴

④ 営業秘密をメール添付で送信した履歴

⑤ 営業秘密をクラウドストレージでコピーした履歴

⑥ 上記の操作をしたパソコンのハードディスクのデータ保全（完全コピー）　　etc…

①～⑤の履歴は、PC操作ログ監視ツールを導入していれば対応が可能です。万が一導入していない場合には、サーバーやプリンター等個別機器のログを精査できます。

4-2. ＜発覚・対策＞フォレンジック調査

さらに、証拠能力・証明力を確保するためフォレンジック調査（退職者のパソコンデータ復元解析）をすることで発見します。 操作ログ監視ツールを導入している場合も、ツールで収集した操作ログと実際のパソコンに残るデータの痕跡が一致していることを証明するために、フォレンジック調査を行います。 退職社員が引き起こす不正は、退職後しばらく経ってから発覚することが多く、すでに各種の履歴が残っておらず、不正を立証するためのデジタル証拠が揃わないという事態に陥りがちです。そのようなときのためにも、⑥のハードディスクのデータ保全によって、各種履歴をフォレンジック調査ができるように、退職時にデータを保存し確保しておくことが重要です。

4-3. 現場社員と管理者（経営者）の認識ギャップ

内部関係者による情報漏えいは、退職というタイミングに限らず、普段から対策を実施していくことが重要です。以下の表は現場社員と経営者や管理者との認識のズレがわかる調査結果です。

4-3-1. 内部不正への気持ちが低下する対策

防止に向けた調査内容ですが、**社員の回答結果では内部不正への気持ちが低下するものとして、PC操作ログ含め、1位：システム操作の証拠が残る（54.2%）に対して、管理者（経営者）では19位（0%）**となり、両者に認識のギャップがあることがわかります。

内部不正への気持ちが低下する対策

社員の回答結果			経営者、管理者の回答結果	
順位	割合*1	対策内容	順位	割合*2
1位	54.2%	社内システムの操作の証拠が残る	19位	0.0%
2位	37.5%	顧客情報など重要な情報にアクセスした人が監視される（アクセスログの監視等含む）	5位	7.3%
3位	36.2%	これまでに同僚が行ったルール違反が発覚し、処罰されたことがある	10位	2.7%
4位	31.6%	社内システムにログインするためのIDやパスワードの管理を徹底する	3位	11.8%
5位	31.4%	顧客情報などの重要な情報を持ち出した場合の罰則規定を強化する	10位	2.7%

*1:内部不正への気持ちが低下すると回答した回答者の割合（社員n=3,000、経営者・管理者n=110）
*2:効果が見込める対策と回答した回答者の割合

（出所）情報処理推進機構（IPA）「組織内部者の不正行為によるインシデント調査報告書」

4-3-2. 内部不正の気持ちを高める要因

以下図は動機や職場環境、スキル(知識・経験)等が原因で内部不正が起こることが考えられるアンケート調査結果です。社員の生の声です。ご参考にしてください。

表 33 社員向け3つの要因に関するアンケート結果（上位３位）

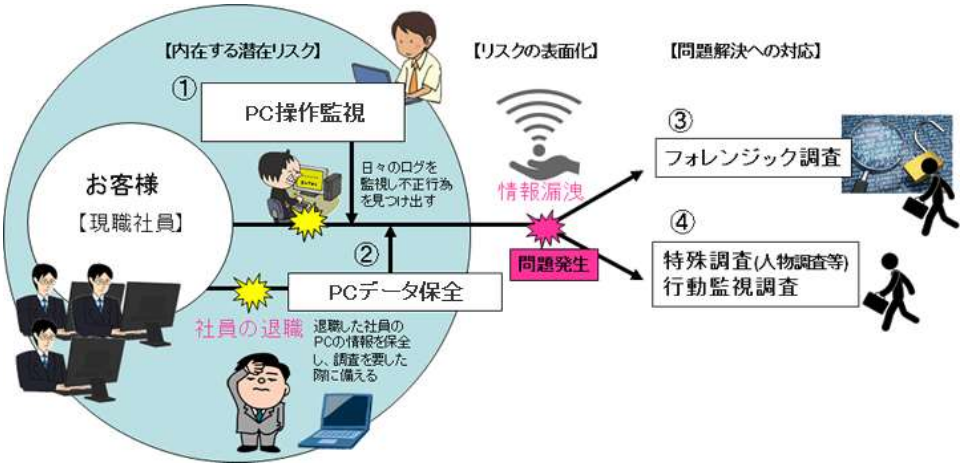
	順位	内容	割合※
動機・プレッシャー	1 位	不当だと思う解雇通告を受けた	30.0%
	2 位	条件のいい企業に対して有利に転職ができる	10.2%
	3 位	社内の人事評価に不満がある	8.2%
環境・機会	1 位	職場で頻繁にルール違反が繰り返されている	8.8%
	2 位	社内ルールや規則を違反した際、罰則がない	8.7%
	3 位	システム管理がずさんで、顧客情報を簡単に持ち出せることを知っている	8.4%
知識・経験	1 位	自分が情報システムの管理者ではないが、不正操作した証拠を消去することができる	9.8%
	2 位	社内の誰にも知られずに、顧客情報などの重要な情報を持ち出せる方法を知っている	9.5%
	2 位	これまでに顧客情報などの重要な情報を持ち出しても誰からも注意や指摘を受けなかった	9.5%

※内部不正行為への気持ちが高まると回答した回答者の割合。

（出所）独立行政法人情報処理推進機構　組織内部者の不正行為によるインシデント調査　（2012年7月）

5. まとめ

弊社では、“人”にフォーカスした総合的な営業機密等の情報漏えいリスク対策の観点から、内部からの情報漏えい防止、または漏えい後をサポートする次のようなソリューションをご提供しております。



5-1. 退職予定者対策

① PC操作ログ監視（※USBメモリ履歴、印刷機監視、クラウドストレージコピー監視含む）

② PCデータ・ハードディスク保全

5-2. 退職後または問題発生後の対策

③ PCデータ解析（フォレンジック調査）

④ WEB監視（各種SNSでの言動調査）

⑤ 行動監視調査（人物調査等）　etc...

これから情報漏えい予防対策を考えている企業様も、改めて強化見直しを検討されている企業様も、いざというときのために最低限のセキュリティ構築及び組織としての整備や準備をすることをおすすめ致します。

不正・不祥事の調査会社をお探しならばこちらへご相談を

社員不正の実態解明には外部の調査を使わなければならないケースが多くあります。

１９６５年創業の総合調査会社 株式会社トクチョーは

※取材による素行調査

※尾行調査（行動監視調査）

※パソコンのログ収集、フォレンジック調査

など充実の調査メニューにてお客様の問題解決に貢献しております。

ご相談・お見積は一切費用を頂戴しておりません。

調査のご検討の際は、まずはお気軽にご相談をしてみてください。

株式会社トクチョー