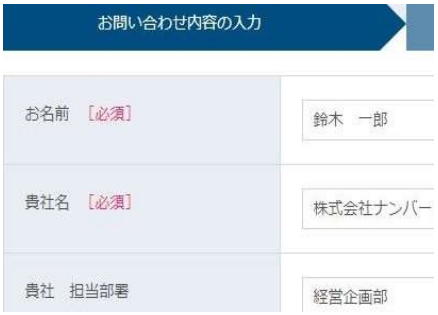
個人情報漏洩のダメージは甚大！発生原因と損害状況、防止策を解説

2018/02/09

『情報セキュリティインシデントに関する調査報告書（2017年6月）』によると、**年間の漏えい件数は報告されただけで約500件**近くにのぼり、その**賠償額の総額は数千億円**にも及んでいます。まるで1つの市場が出来上がるようなインパクトがあります。**漏えいする原因の約70%が管理不足や誤操作、紛失等の悪意のないもので日々の日常業務に原因**が潜んでいます。悪意がないとはいえ、決して他人事では済まない経済的リスクがあることを認識していただくためにも、本稿では情報漏えいに対する原因と対策の説明とともに、想定賠償額の計算方法にも触れることで具体的な経済的リスクを把握して頂ける内容を紹介します。また外部からの不正アクセスや内部不正などによる原因も一定の割合で存在していることも事実です。こうした不正による情報漏えいをどのように防いでいくかという不正防止策についてもご紹介します。



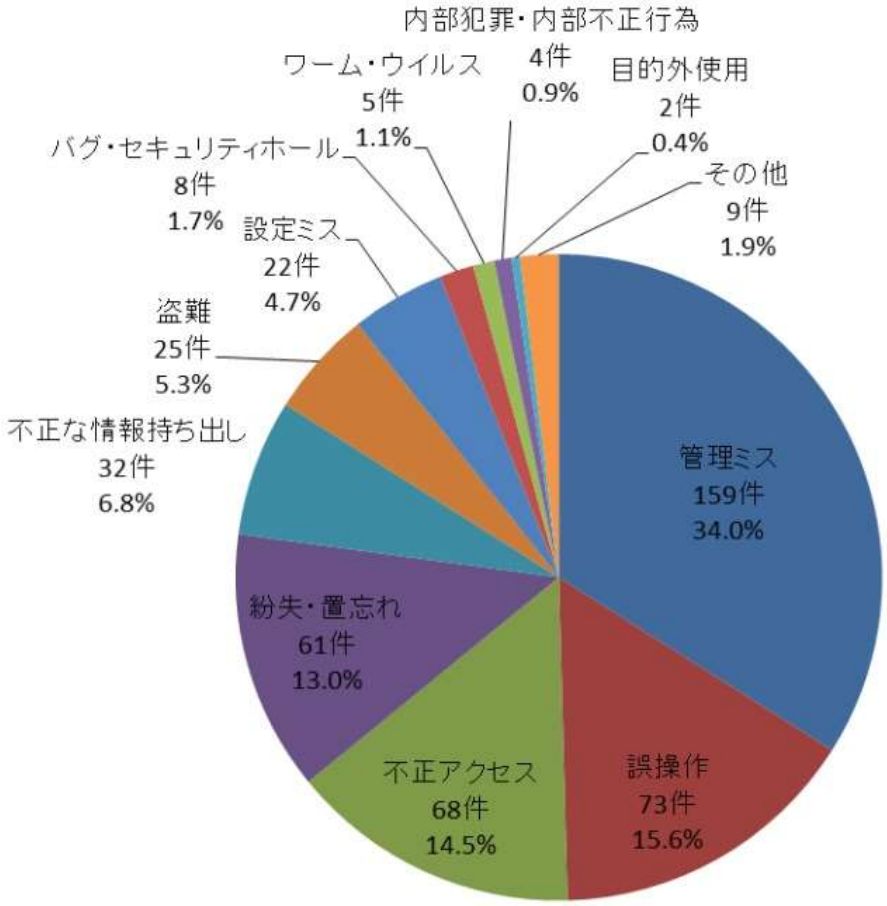
※【参考】JNSA2016年情報セキュリティインシデントに関する調査報告書（2017年6月）」

目次

1. 情報漏えいの原因　ワースト5位
　1-1. 『管理ミス』を防ぐ対策
　1-2. 『誤作動』を防ぐ対策
　1-3. 『紛失や置忘れ』を防ぐ対策
2. 個人情報漏えい時の想定賠償額
　2-1. 年間賠償額合計は約3,000億円
　2-2. 被害者1人あたりの平均損害賠償額は　3万円
　2-3. 実際の賠償額計算方法
3. ＜社外＞不正から起こる情報漏えい防止策
　3-1. 不特定外部者からの不正アクセスからの防止策4つ
　3-2. 取引先からの流出を防ぐ対策/a>
4. ＜社内＞不正から起こる情報漏えい防止策
　4-1. 不正持ち出しによる流出
　4-2. （参考）内部不正への気持ちが低下する対策
　4-3. （参考）内部不正の気持ちを高める要因
5. まとめ

1. 情報漏えいの原因　ワースト5位

以下の図をご覧ください。ワースト1位：管理ミス（34%）、2位：誤操作（15.6%）、3位：不正アクセス、4位：紛失・鍵忘れ（13%）、5位：不正な持ち出し　の順番となります。ただし特に「1位：管理ミス」、「2位：誤操作」、「4位：紛失・鍵忘れ」という日常業務においての防止チェックや体制構築で、多くの情報漏えいを未然に防ぐことができます。まずは上記3つの日常業務における具体的な防止策作りを説明します。



【漏洩原因比率】

※特定非営利活動法人日本ネットワークセキュリティ協会「2016年 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～」p12より引用

1-1.『管理ミス』を防ぐ対策

ここでは、管理者として組織的に見直す対策について触れてみたいと思います。

1-1-1. 情報資産の厳重保管について

- 責任者が施錠管理を行なう
- 専用スペースを設置し分別をして保管とともに無断開閉をなくす
- 入退室記録の設置
- 廃棄時は復元不可能な状態にする（シュレッダー等）
- 個人パソコン等からの社内ネットワーク接続の禁止

1-1-2. 秘密情報の定義と表示及び取り扱いルールをつくる

- どの情報が「オープン」「社外秘」「極秘」なのかを経営側でしっかりと定義する
- 情報ごとに従業員にわかりやすく表示する、また周知を行なう
- 情報ごとに取り扱いに関するルールと罰則を決める
- 内部通報窓口、または社外通報窓口の設置

1-2.　『誤作動』を防ぐ対策

誤操作のうち特に大きな割合を占める“メールにおける”誤操作防止策をお伝えします。

従業員1人1人の心構えも大切ですが、意識に頼らない設定テクニックなどもありますのでご紹介します。

▪ メール送信ボタンとともにメールを送らない
メールを送信トレイに一度おく方法です。確実に送るには送受信ボタンを押すか、そのメールの送信ボタンを押さなくては送られません。送る前に1度送信先アドレス等の再確認ができる方法です。

▪ 「自動補完（オートコンプリート）機能」を解除する
アドレスを入力する際に、送ったことのあるアドレス等が自動的に表示されてしまうものです。
アドレス入力の手間が省けるメリットがありますが、送りたい相手ではないアドレスが表示されることもあるため設定後に1度確認しない場合は、送信ボタンを押したが最後、対象外の相手に送られてしまい情報が漏えいすることになります。

▪ どんな添付ファイルにも暗号をつける
最低限ですが、特に大切な資料や機密情報であればあるほど、添付資料には暗号をつけて送るようにしましょう。

1-3. 『紛失や置忘れ』を防ぐ対策

▪ 持ち出しや複製、複写は原則として禁止にする、または情報責任者の許可制とする

▪ 持ち出しの際は鍵付き鞄やGPSなどで紛失場所が特定できるような工夫をする

▪ パソコン、スマートフォン、UBSメモリ等の持ち出しを禁止、または許可制とする

2.　個人情報漏えい時の想定賠償額

顧客情報などが漏えいした場合、どのような経営リスクとなる経済的なコストがのしかかってくるかについての算出方法をご紹介します。社員たった1人のミスが命取りになるような多大なるコストを発生することをご覧頂ければと思います。

2-1. 年間賠償額合計は約3,000億円

2017年版のJNSA情報セキュリティインシデントに関する調査によれば、2016年の年間賠償額は約3,000億円（2,788億7,979万円）という結果がありました。 2004年の大手通信企業で起きた情報漏えいでは、451万件分の顧客情報が流出しましたが、お詫びは500円の金券とメール・アドレスの無料変更でした。また2014年に起きた大手教育企業での情報漏えいが問題になりましたが、その際の**被害者1人あたりに配られた “お詫び”（500円の電子マネーやQUOカード）などが記憶に新しいかと思いますが、万が一御社で事態が起きた場合、そのような対応で済むとお考えでしたら改めて頂きたい**と思います。

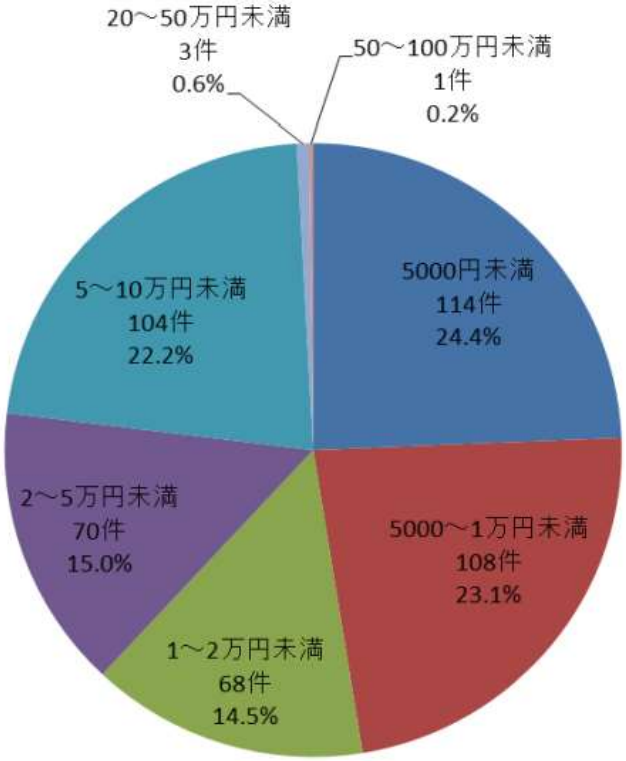
漏えい人数	1,396 万 5,227 人
インシデント件数	468 件
想定損害賠償総額	2,788 億 7,979 万円
一件あたりの漏えい人数※1	3 万 1,453 人
一件あたり平均想定損害賠償額※1	6 億 2,811 万円
一人あたり平均想定損害賠償額※2	3 万 1,646 円

【2016年 個人情報漏えいインシデント概要データ】

※特定非営利活動法人日本ネットワークセキュリティ協会「2016年 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～」p6より引用

2-2. 被害者1人あたりの平均損害賠償額は　3万円

以下の図は被害者個人が受け取った損害賠償額の件数比率になります。被害者１人あたりの平均損害賠償額は3万円ほどです。年間事故件数約500件の全体から見ると先にご紹介した大手企業の賠償額500円がどれほど現実離れしているかがわかります。図をご覧頂くと、**賠償額5,000円（0が1つ増えます）未満の件数はわずか24.4%**に過ぎません。つまり**1人あたり5,000円以上が実に75%以上近くを占めている**のです。



【一人当たりの想定損害賠償額比率(件数)】

※特定非営利活動法人日本ネットワークセキュリティ協会「2016年　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～」p28より引用

それでは、その年度という定点観測ではなく、約10年にわたり平均一人当たりの想定損害賠償額が調査結果にありました。以下の図になりますが、あくまでも平均値ではありますが、2万円後半から5万円の間を行ったりきたりしているのが現状なのです。

	想定損害賠償総額
2005 年	4 万 547 円
2006 年	3 万 6,743 円
2007 年	3 万 8,228 円
2008 年	4 万 3,632 円
2009 年	4 万 9,961 円
2010 年	4 万 2,662 円
2011 年	4 万 8,560 円
2012 年	4 万 4,628 円
2013 年	2 万 7,675 円
2014 年	5 万 2,625 円
2015 年	3 万 4,058 円
2016 年	3 万 1,646 円

【一人当たりの平均想定損害賠償額】

※特定非営利活動法人日本ネットワークセキュリティ協会「2016年　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～」p28より引用

2-3. 実際の賠償額計算方法

それでは、先述しました1人あたりの500円の賠償額含め、どのような算出をしているのでしょうか。

その方法として一般的に業界で用いられる「JOによる計算モデル」と「損害保険サービスでの補償額」の2つから考察してみたいと思います。また後者の保険サービスでは賠償額だけではなく、その各種マスコミ対応、詫び状送付等の実務にかかる2次費用などもご参考にしていただけるのではないかと思います。

2-3-1. JOモデルによる損害賠償額の計算

計算図が出てくると難しいと考え避けてしまうところですが、内容は至ってシンプルですので　どうぞお付き合いください。

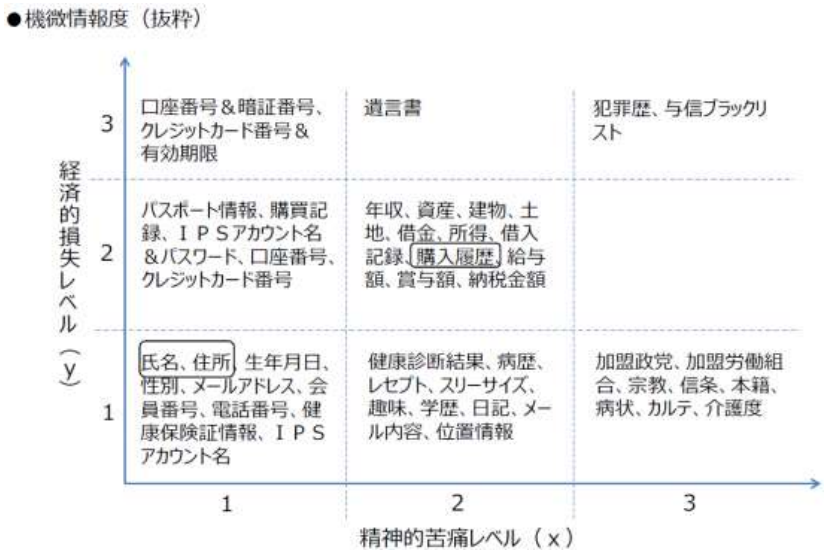
日本ネットワークセキュリティ協会（JNSA）では、個人情報漏えいにおける損害賠償について、過去の事件・事故の分析・プライバシー権や名誉棄損の判例分析等に基づき、独自の想定損害額算出モデルである「（JINSA　Damage Operation Model For Individual Information Leak）」を発表していますので参考例をもとにご紹介します。

（参考例）一般企業において、氏名、住所、購入履歴のあるデータが漏えいした場合1人あたりの倍業額は以下の式で求められます。

賠償額＝①基礎情報額×②機微情報度×③本人特定容易度×④社会的責任度×⑤事後対応評価

①基礎情報額･･･基本的な情報の値段です　500円と設定されています

②機微情報度･･･以下の図にある経済的損失、精神的苦痛レベルの内容でXとYのいずれか大きい方の数字を選択します



※□印は今回漏えいした項目を示しています

③本人特定容易度･･･どの程度特定されうるかという指標を当てはめます

● 本人特定容易度

判定基準	本人特定容易度
個人を簡単に特定可能。「氏名」「住所」が含まれること。	6
コストを掛ければ個人が特定できる。「氏名」または「住所・電話番号」が含まれること。	3
特定困難。上記以外。	1

④社会的責任度･･･中小企業は以下の「一般的」に属する場合がほとんどです

● 社会的責任度

判定基準	社会的責任度
一般より高い：適正な取り扱いを確保すべき個別分野の業種〔医療、金融･信用、情報通信等〕及び、知名度の高い大企業、公的機関	2
一　般　的　：その他一般的企業及び、団体・組織	1

⑤事後対応評価･･･発生後の対応姿勢についての評価を当てはめます

● 事後対応評価

判定基準	事後対応評価	適切な対応行動例	不適切な対応行動例
適　　切	1	素早い対応、被害状況の把握、インシデントの公表、状況の逐次公開、被害者に対する謝罪、クレーム窓口の設置、漏洩情報の回収、顧客に対する補償、原因の追究、セキュリティ対策の改善	指摘されても放置したまま、対応が遅い、繰り返し発生、対策を施したが有効でない、虚偽報告
不 適 切	2		
不明、その他	1		

上記①～⑤を計算式に当てはめますと下記の様な積算となります。

【損害賠償額計算例】

▪ 一般企業において、氏名、住所、購入履歴のあるデータが漏洩した場合の賠償額

１人あたりの賠償額：　５００　〔基礎情報額〕
×１０$^{2-1}$＋５$^{2-1}$〔購入履歴の機微情報度:ｘ=2、ｙ=2〕
×６　〔本人特定許容度〕
×１　〔社会的責任度:一般企業〕
×１　〔事後対応適切度〕

＝**４５，０００円**

▪ 漏洩件数：１０，０００人とすると

４５，０００円 × １０，０００人　＝　**４億５，０００万円**

※実際には、個人情報を漏洩された全員が訴訟に参加するわけではありません。正式なデータは存在しませんが、訴訟参加率は0.5～5％程度でシミュレーションされることが多いようです。

機微情報度は住所･氏名はｘ=1、y=1 ですが、購入履歴はｘ=2、y=2 であるため、大きい数値である購入履歴の数値を採用します。

※「（引用）銀泉リスクソリューションズ㈱ RISK SOLUTIONS REPORT 2015」

2-3-2. 情報漏えい保険商品からみる想定賠償額

日本商工会議所が運営する保険制度サイト（ https://hoken.jcci.or.jp/compromise）には、会員向けですが情報漏えいに関する一般的な保険サービス内容（情報漏えい賠償責任保険）が、大手6社の損害保険会社の紹介とともに確認できます。一般的な例として以下の内容を保険でカバーすることが記載されていました。賠償額だけでなく、その後の訴訟費用や実務費用などにも補償が設けられております。ご参考までに取り上げてみます。一部省略しております。

▪ おすすめ1：外部起因・内部起因の事故を幅広くカバー

▪ おすすめ2：サイバー攻撃等の際の対応費用を手厚く補償

▪ おすすめ3：見舞金・見舞品購入費用も補償

▪ おすすめ4：海外で訴訟提起された損害賠償請求も補償

▪ おすすめ5：充実した補償のほか、事故対応等のサービスをご提供

（補償例）10万件の個人情報が漏えいした場合 → 総額1億7,370万円の損害に！

〈事故発生時の保険金支払例〉

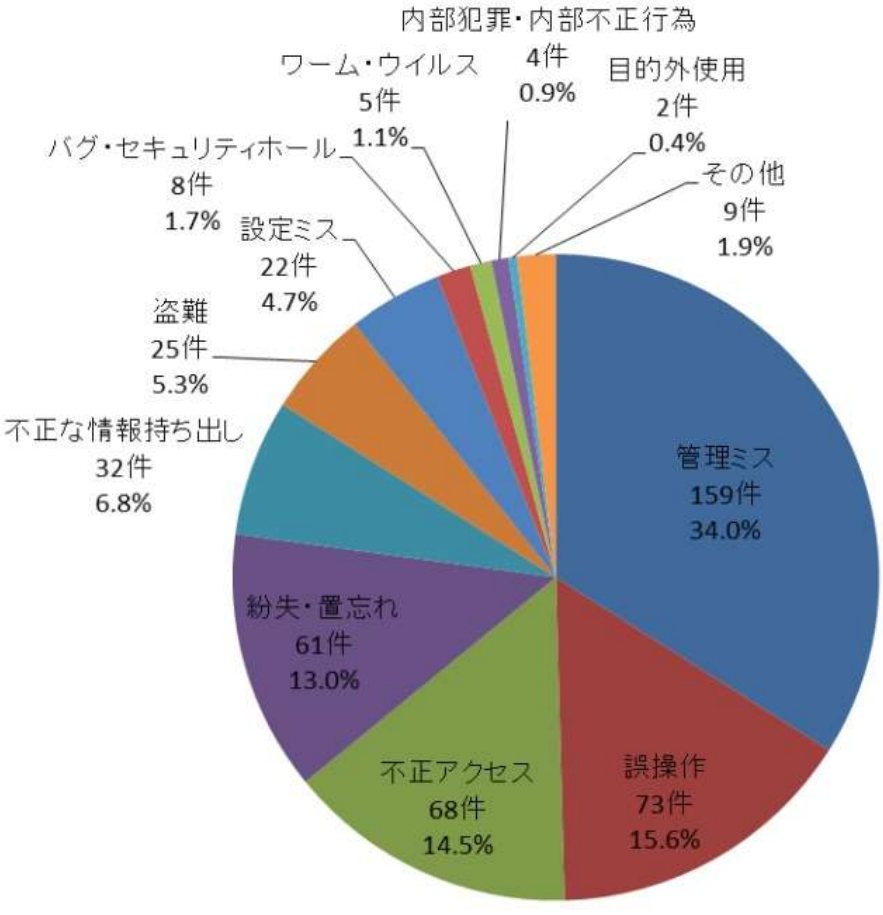
項目	被害想定金額	補償の可否
賠償損害	5,600万円	賠償損害として補償
争訟費用	300万円	
詫び状発送	1,200万円	
お詫び掲載	100万円	
新聞社告	1,800万円	
見舞金	8,120万円	
コールセンター	850万円	
法律相談	100万円	
原因調査費用	1,000万円	
データ復旧	300万円	
合計	1億7,370万円	

※上記被害想定金額は、仮定のもとに算出した簡易試算の結果です（上記サイト注記より）

3. ＜社外＞不正から起こる情報漏えい防止策

ここでは特に社外からの不正なアクセスや持ち出しなどによる情報漏えいについての防止策をご紹介します。
1.情報漏えいの原因ワースト5の図を再度ご覧ください。

情報漏えい原因比率の第3位が不正アクセス（14.5%）、また5位が不正な情報の持ち出し（6.8%）となり、社外からの原因で起こる情報漏えいは約2割です。決して侮れません。この2つの原因に対する防止策を“不特定外部”と“取引先”の2つに分けてご紹介します。



【漏洩原因比率】

※特定非営利活動法人日本ネットワークセキュリティ協会「2016年 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～」p12より引用

3-1. 不特定外部者からの不正アクセスからの防止策4つ

特にネットからの不正アクセスに対する防止策をご説明します。

3-1-1. 外部ネットワークにつながない機器に秘密情報を保存する

不正アクセス等に備え、ネットワークに接続された機器で利用・保管する必要性のない秘密情報については、その利用態様を踏まえ、外部ネットワークにつながない機器に保存することが有効です。

3-1-2. ファイアーウォール、アンチウィルスソフトの導入、ソフトウェアのアップデート

ネットワークにつながったＰＣ等の機器に保管されている秘密情報を不正アクセス等から守るためには、ファイアーウォールの導入や、ウィルスに感染させないためのアンチウィルスソフトなどのセキュリティソフトの導入、各種ソフトウェアの適時のアップデートが重要です。さらに不正侵入防御システムの導入等により防御することも有効と考えられます。

3-1-3. 不特定外部者からの標的型攻撃メール対策

情報窃取活動への対抗手段として、まずは社内における秘密情報へのアクセス権者を最小限にする対策が有効となります。

3-1-4. ネットワークの分離（複数のLANを構築）

ネットワークを分離することで、1つのネットワークに不正アクセス等があった場合でも、その他のネットワークに保管される秘密情報へは直接アクセスできないため、接近の制御の強化とともにウィルス等に感染した場合でも被害の拡散防止にもなります。またVPN（バーチャルプライベートネットワーク）を適切に活用することで、安全性を担保しつつネットワーク構築に柔軟性を持たせることができるようになります。

3-2. 取引先からの流出を防ぐ対策

自社の秘密情報を共有する相手方を指します。例えば、委託先や委託元、外注先や外注元、共同研究先または日常的にオフィスに出入りする業者等が考えられます。取引先を通じた情報漏えいの中には、大別して、以下の２つのパターンが考えられます。

▪ 取引先自体が主体となり悪意で情報の不正使用や不正開示を行う場合

▪ 配達業者ほか人的にオフィスへ出入りする業者による不正流出する場合

以下それぞれの対策をご紹介します。

3-2-1. 取引先自体が主体となり悪意で情報の不正使用や不正開示を行う場合

委託先の情報管理能力を確認する際に参考となる基準としては、ISMSが代表ですが、その他には、例えば、内閣サイバーセキュリティセンター（NISC）が政府機関向けに策定している『政府機関の情報セキュリティ対策のための統一基準（平成２６年度版）』のP.23以降に、政府機関が外部委託する場合のセキュリティ基準が掲載されているので参考になるでしょう。また、今後は委託先の業務従事者の中に「情報セキュリティマネジメント試験」の有資格者（平成28年度春期から開始）がいるかどうかといった観点などは双方にとって信任されやすいものと思われます。なお、秘密情報の開示に当たっては、事前に秘密保持契約を締結することが前提です。

3-2-2. 機器メンテナンス等、自社の秘密情報に接する可能性のある業務を外注する場合

秘密情報を保管する建物や部屋の入場制限や入退場チェック、書棚や媒体、システム等のアクセス制限を実施します。具体的には、

▪ 敷地入口での警備員による身分確認。

▪ 入構ゲートを設置し、ID認証での入構制限。

▪ 書類・ファイル、記録機器・媒体を保管する区域を施錠管理し、入退室を制限。

（例）書庫、サーバールームなど

各種メンテナンス業者等、一定の許可の下に、秘密情報に接する可能性のある事業者に対しては、「業務中に接する一切の情報を漏えいしてはならない」旨を業務委託契約等に盛り込むこと等が大変重要です。

3-2-3. 配達業者ほか人的にオフィスへ出入りする業者による不正流出する場合

ルートを適正に限定し、従業員が同行の上、秘密情報が保管されたエリアや部屋には近づけないようにすることが有効です。受付窓口より先に入室させず、外で受け取るなどの対応が必要です。

3-2-4.（参考）入構時の基本対応

入口にて来訪者カード等を準備し、氏名や訪問先を記入してもらい、アポイントの有無を確認することなどにより、来訪者に対し情報管理に係る関心が高く、管理が行き届いた職場であると認識させ不正行為を心理的に抑制します。また、来訪者の入構時には、当該来訪者と実際に面識のある従業員が直接入口に出迎えることによって来訪者のなりすましを防ぎます。入構の際に、来訪者用のバッジ等を渡して着用してもらうことで、その者が来訪者であるということが外見上明らかとなり、従業員等の意識的又は無意識的な関心を集め不正行為に対して心理的な抑止効果が期待できます。

4. ＜社外＞不正から起こる情報漏えい防止策

4-1. 不正持ち出しによる流出

→営業秘密情報漏洩の記事を参照ください。

【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】

4-2.（参考）内部不正への気持ちが低下する対策

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。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.（参考）　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

【悪意のない】日常業務の中で起こる単なるミスによる情報漏えいと言えども

▪ 多額な経済的コストがかかること（➡ 2. 個人情報漏えい時の想定賠償額　）

被害者一人あたり5千円以上が全体の事故件数の75%を占めており、世間一般で目にしている賠償額（被害者：500円/人）では収まらないケースがほとんどです。
さらに、

▪ 悪意ある不正アクセス（社外）や不正な持ち出し（社内外）による攻撃にも備えをすること

を念頭において頂ければ幸甚です。

起きてから大問題に発展するこうした経営リスクこそ、**転ばぬ先の杖として特に経営者や管理者の皆様には日々備えて頂きたいと思います。**

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