Available Information Report for Corporate Management

経営情報レポート

情報漏洩はトータルな対策が重要

歯科医院の個人情報漏洩対策

1. 個人情報漏洩の現状
2. 個人情報漏洩対策
3. 就業規則・労働契約書の整備による事前防止策

中央税務会計事務所

1 ｜ 個人情報漏洩の現状

IT 環境の進化に対し、環境の整備やスタッフへの周知徹底が図られていないために、ＰＣやＵＳＢの紛失、不正アクセスによる情報漏洩が発生しています。また、スタッフがツイッターで診療所の悪口を書き込むなど、今までとは異なった新たな媒体に対する防止策が必要となっています。

本レポートでは、情報漏えいの現状と、医療従事者に課せられる守秘義務及び個人情報保護法について考えます。

1 ｜ パソコン、USB 等からの情報漏洩の現状

今年、ベネッサや東京電力等での情報漏洩事件・事故が騒がれました。これらの事件は、毎年増加しており、医療機関及び関連業者においても情報漏洩事件が多発しています。

■医療機関関連の情報漏洩事件・事故（平成 26 年６月以降分）

●T 歯科診療所・・・外来患者のカルテ等の紛失
●S 歯科クリニック・・・患者情報が保存されたＰＣが盗難被害
●医療向け転職サイトの元従業員・・・Ｄｒ、看護師の個人情報を持出し、逮捕
●兵庫医科大・・・個人情報を含むファイルを学生 125 人へメール送信
●A 市の民間病院・・・健診受診者の個人情報含むＵＳＢを紛失
●大分大付属病院・・・患者個人情報入りＵＳＢが所在不明
●協会健保兵庫・・・被保険者証の返納依頼文に誤って別家族名を記載し送付
●福島県総合療育センター・・・患者情報 682 件を含むＵＳＢが所在不明
●新潟県立病院・・・外来患者カルテを清掃職員が誤って回収、廃棄処分
●都立広尾病院・・・研修医が患者情報をＵＳＢに無断コピーし、紛失

出典：当社情報及びインターネットＳｅｃｕｒｉｔｙＮＥＸＴ　個人情報漏洩事件・事故一覧

これらのほかにも、多数の病院、診療所、歯科診療所において盗難や紛失による情報漏洩につながる事件事故が起きています。多くがＰＣやＵＳＢメモリの紛失や盗難によるものです。また、この他にコンピュータウイルス（サイバー攻撃）によってＰＣから情報を送信させるといった手口の事件も起こっています。

■ＰＣウイルスの種類

１．自己増殖

インターネットやＬＡＮを使用して、他の多くのＰＣに感染する目的のウイルスがある

「ワーム型」・・自分自身の複製を電子メールの添付ファイルとして送信し、ネットワークドライブに保存されているファイルに感染
利用者の操作を介さず、自動的に増殖

２．情報漏洩

- ＰＣに保存されている情報が外部の特定サイトに送信されて起こる場合
- インターネット上に情報が広く公開されて起こる場合
- キーボードで入力した情報を記録する「キーロガー」
- ＰＣ内に記録されている情報を外部に送信する「スパイウエア」　　等

３．バックドアの作成

ウイルス感染したＰＣ内部に潜伏するタイプのウイルス「トロイの木馬」と呼ぶ「バックドア」・・・ＰＣの裏口を作成し、外部から自由に操作される（遠隔操作）

４．ＰＣシステムの破壊

ＰＣシステムを破壊してしまうものがある
特定の拡張子を探し、自動停止させるものやＰＣ動作を停止してしまうもの

５．メッセージや画像の表示

いたずらを目的としたウイルス（一定時期を過ぎると特定のメッセージや画像を表示）

２｜インターネット上での歯科医院内部の情報漏洩

個人情報だけでなく、院内で発生した出来事（事故やクレーム等）を、スタッフがブログやツイッター等で掲示することがあります。個人から発せられる情報がインターネット上に出てしまい、悪評になって広がったり、実際は違うのに風評として受け取られたりしています。当人には悪口のつもりがなくとも、受け取り側の感覚・判断で悪評は出来上がってしまいます。

ツイッターやブログ、２チャンネル、ライン等での情報交換は、当人には広げるという意識が無くとも、見る側には伝わりません。また、当人が特定の相手だけに行ったとしても、その相手がまた別の人へ伝えることを防げません。

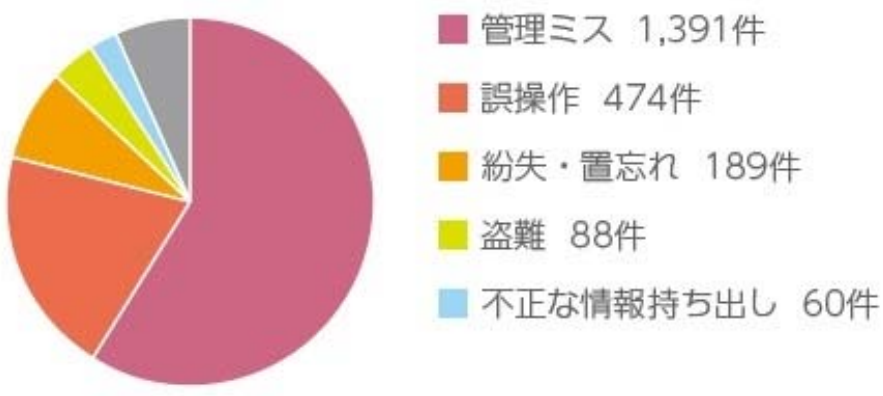
当人のモラルの向上や高い意識を持たせることを医院側から行う必要があります。

3｜情報漏洩の原因

(1)情報漏洩の原因と経路

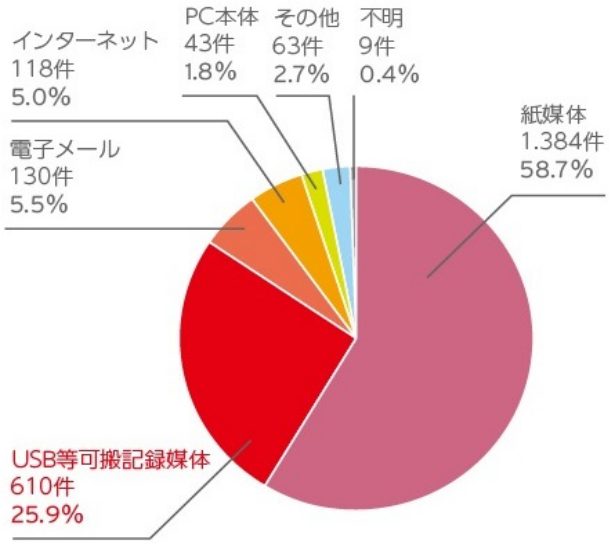
情報漏洩の原因は、管理ミスや誤操作、紛失置き忘れ等のうっかりミスが全体の約９３％を占めています。盗難や外部からの不正アクセス等による漏洩は、６．７％と少ない数値ですが、これらの漏洩は大きな被害を招くことが多く、対策を行うことが重要です。

■情報漏洩の原因



※出典　ＪＮＳＡ2012 年情報セキュリティインシデントに関する調査報告書

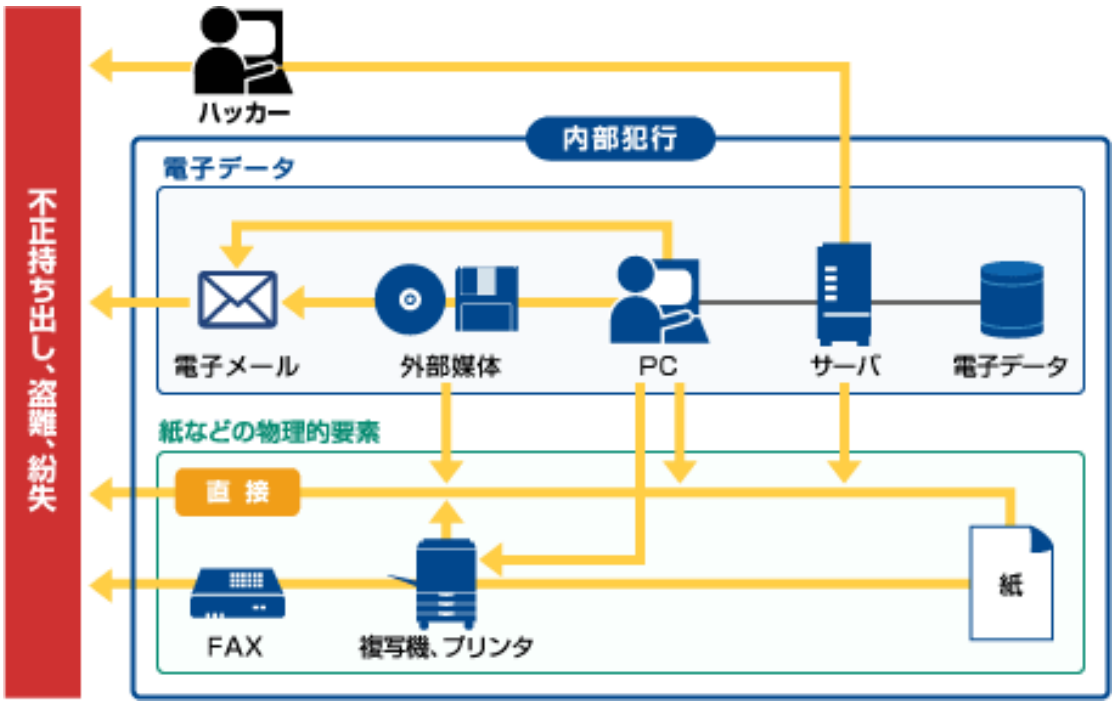
■情報漏洩の経路



※出典　ＮＰＯ日本ネットワークセキュリティ協会 2012 年情報セキュリティインシデントに関する調査報告書

経路別の件数は、紙媒体による漏洩が５８．７％と全体の約 6 割を占めています。漏洩の個人情報の人数は、ＵＳＢなど可搬記録媒体による漏洩が最も多く、2012 年では約 760 万人に及び全体の約 75%になっています。（ＪＮＳＡ2012 セキュリティインシデントに関する調査報告書より）

■内部から漏洩する場合の主な手段と経路



出典：セコムトラストシステムズ（株）　情報漏洩対策サイト

(2)情報漏洩の影響は多大

情報漏洩が起こると、医院は大きな損害を被ります。個別に、情報漏洩してしまった当人への損害賠償費用（謝罪費用も含む）、調査費用といった金額の他、医院としての信頼やイメージの低下等による影響は多大になります。

医院経営が安定するまでの労力・努力が、あっという間に消え去ります。その原因が内部に多く存在しています。

内部要因による情報漏洩を防止するために、院長からスタッフ全員まで、医院全体をあげて対策を講じる必要があります。

2 個人情報漏洩対策

医院内には多数の重要な情報があります。保険証や問診票や患者アンケートといった情報の他、カルテという最重要な情報が存在しています。適切な管理・保管を行う必要があります。情報漏洩対策はセキュリティ製品による制御だけでなく、ルールの明確化やスタッフへの徹底をしなければいけません。また、雇用形態の変化やＩＴ環境の変化によって、定期的にルールや製品の見直し、また定期的なスタッフ教育の実践とモラル向上の研修を行わなければいけません。

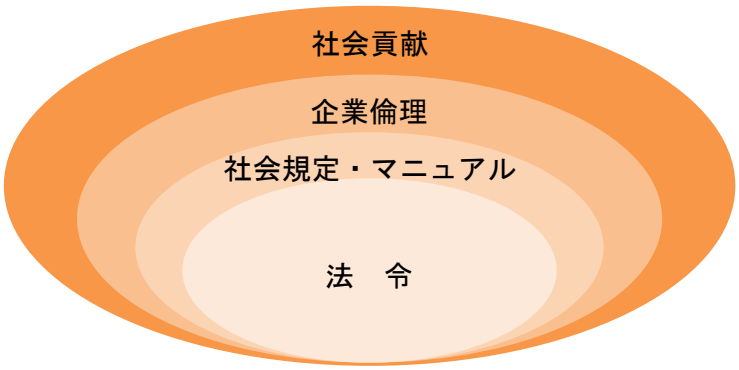
1 院内ルールの明確化

(1)コンプライアンスの考え方

コンプライアンスを『法令遵守』とだけとらえ、法律に違反していないから大丈夫だと考えることは非常に危険です。医院の規模や問題の種類によっては、「法令に違反していない」と説明しても、それが必ずしも患者やその家族が納得できるものとは聞こえないことが多々あるからです。コンプライアンスを原点として、『公正・適切な企業活動を通じ社会貢献を行なう』という思想があります。

医療機関には、他の模範となるべく、積極的に法令や条例以上の倫理・社会貢献を遵守し、『常識が法である』という行動が求められています。

■コンプライアンスの範囲



(2)ガイドライン

厚生労働省からも医療機関に対し、個人情報寳語法としてのガイドラインが発表されています。その趣旨や基本的な考え方に沿って、各医療機関でもガイドラインを作成し、遵守することが重要です。

(3)情報整理

医療機関では、患者さん及びその家族について個人情報を詳細に知りうる立場にあるため、適正な取り扱いが求められています。知りえた情報を整理し、しっかりと管理する必要があります。なんとなくではなく、情報収集方法、管理方法といった基準を作成し、取扱いにまで、制約を求めるべきです。

(4)個人情報保護法と守秘義務

個人情報保護法の中での「個人情報」とは、生存する個人に対する情報とされています。医療関係の情報を対象としていますが、診療録等の形態に整理されていない場合でも個人情報に該当します。なお、当該患者さんが死亡した後においても、医療機関で情報を保存している場合には、漏洩、滅失または毀損等の防止のため、個人情報と同等の安全管理措置を講ずるものとすると、規定されています。

また、医療法の第 15 条において、診療所の管理者は従業員に対する管理監督義務があり、と定められています。歯科医師や歯科衛生士、他医療に関する資格者が守秘義務を負っていることを考えると、医療機関に従事する人は、管理者の監督の下、守秘義務も遵守しなければならないと解釈されています。

■医療関係資格者に係る守秘義務

資格名	根拠法
歯科医師	刑法第 134 条第 1 項
薬剤師	刑法第 134 条第 1 項
歯科衛生士	歯科衛生士法第 13 条の 5
歯科技工士	歯科技工士法第 20 条の 2

2｜ツールによる対策

(1)デバイスコントロール

アクセスコントロールの設定によって、外部デバイスへのユーザアクセスを制御することが可能です。制御可能なデバイスは、以下のとおりです。

■制御できるデバイス

ＵＳＢ型通信デバイス	モデム。電話など
ＵＳＢプリンタ	USB ケーブルを使ってパソコンとプリンターを接続する方法。

ＵＳＢデータストレージデバイス	パソコンから記憶装置と見えるもの、ハードディスクやリムーバブルディスクと表示されるもの
ＣＤ／ＤＶＤ－ＲＯＭデバイス	ＣＤ/ＤＶＤディスクの読書きを行う光デバイスを含む
ディスクドライブ	ＨＤやＦＤ上のデータを読書きするデバイス
モデム	通信システムで使用されるデバイス、ダイヤルアップ、ＡＤＳＬ、イーサネットモデムを含む
ストリーマ	磁気テープ上のデータの読書きを行うデータストレージデバイス
入力デバイス	デジタルカメラ、スキャナなどのデバイスを含む
赤外線デバイス	赤外線ポート経由で CP に接続するデバイス
MTB デバイス	フラッシュカード等のデータストレージデバイス
多機能デバイス	ストレージやメモリカードリーダ、PCMCA モデムなどの複数の機能を一体化したデバイス
スマートカードリーダ	プリペイドカード、クレジットカード等あらゆる種類のスマートカードを含む

(2)アーカイブ／ログ監査

アーカイブとは重要記録を保存・活用し、未来に伝達することをいいます。一般的に書庫や保存記録と訳されますが、PC 上のデータの世代管理を行う上でデータとメタデータを合わせて保管することをアーカイブファイルと呼びます。他にウエブを収集したウエブアーカイブ、デジタル化して保存するデジタルアーカイブと呼ばれるものがあります。

ログ監査を行うことは、各種 PC の捜査記録を監査証跡として取得することになります。その上で、監査証跡を利用者に還元し、追跡できる環境を整備することで牽制効果が表れ、利用者に不正やルール違反をさせない事につながります。

(3)コンテンツフィルタリング

好ましくないウエブサイトなどが閲覧できないように、クライアントもしくは内部サーバで走るソフトウエアによって、閲覧内容に一定の規制を掛ける仕組みです。教育・倫理上の問題や医院内での行動規範の問題を背景として、製品化されています。

(4)URLフィルタリング

ネットワークや PC からアクセス・閲覧できるインターネット上のウエブサイトを制限する方式の一つで、閲覧を許可する（あるいは拒否する）URL を列挙する方式、又はそのような方式で閲覧制限を行うソフトウエアやソフトウエアの機能のことをいいます。

3｜スタッフ教育の徹底

(1)スタッフのモラル、メディアリテラシーの向上

情報漏洩は、悪意の無いうっかりとか誤操作によるものと故意によるものがあります。マニュアルによる行動管理やシステムによる制御も大事ですが、基本はスタッフ自身のモラルの向上が必要です。また、メディアリテラシーという「情報を評価・識別する能力、情報を発信する能力」を向上させ、本来の目的を認識したうえで活用することが重要となります。

(2)定期的なスタッフ教育

歯科医院において、個人情報保護に対する体制・諸規定を整備し、スタッフに対する研修を実施し、教育を行うことが重要なポイントです。医療安全対策や院内感染防止対策の研修会に関しては年 2 回以上の研修会の開催と規定されています。併せて行うことが望ましいでしょう。

①組織体制の整備

- ●個人情報の保護に関する委員会の設置
- ●個人情報保護管理者の任命（院長兼任で可）
- ●個人情報の取扱いに関する苦情処理を行う窓口機能の整備
  （窓口は院長で可・従業員への周知徹底）

②個人情報に関する諸規定の整備

- ●個人情報保護に関する方針の作成
- ●個人情報保護に関する規定の作成
- ●個人情報の開示に関する手続きの定め
- ●個人情報漏洩時の対応手順（マニュアル）の作成
- ●個人情報の取扱いに関する苦情対応の手順（マニュアル）の作成
- ●雇用契約書等に離職後も含めた守秘義務の規定整備
- ●業務委託契約書等に安全管理措置、受託者の義務規定等の明記

③スタッフに対する研修の実施

- ●従業者に対する研修を実施する

3 就業規則・労働契約書の整備による事前防止策

スタッフが 10 名未満の歯科医院では就業規則の作成は義務化されていませんが、個人情報漏洩では監督者である院長が法律によって罰せられることも有るため、就業規則・その内部の服務規程、労働契約書等に、個人情報漏洩に関する基準や考え方を明記し、スタッフへ通達することが必要です。

勤務歯科医師や歯科衛生士は資格取得する際に、守秘義務として研修していますが、受付、歯科助手、歯科医療事務といった無資格者（民間の認定資格者）は守秘義務を知らないことが多く、その認識の甘さから漏洩につながることが少なくありません。

1 医療法による個人情報保護法のガイドライン

(1)歯科医院における個人情報の種類と医療法によるガイドライン

歯科医院においては、保険証を預かり、カルテを作成し、問診表にまで記入してもらいます。院内ではＸ線装置で口腔内の撮影をし、フィルムもしくはデータにて保管しています。また、診療報酬請求に際しては、審査支払機関へのレセプトの提出があり、他の事業者へも常時情報提供をしています。健康診断を行えば、勤務先（事業者）へ従業員の健康診断結果を通知します。技工所への技工指示書等によっても個人情報の提供があります。

このように、色々な状況で個人情報に触れ、他に提供しているのが歯科医院です。当然歯科医院側に、個人情報保護・管理の取り組みが必要となります。

■医療法のガイドライン

●医療関係事業者の利用目的の特定及び制限

患者から個人情報を患者に対する医療の提供、医療保険事務、入退院等の病棟管理などで利用すること以外で利用する場合は、明確に当該利用目的を公表等の措置が講じられなければならない

●責任体制の明確化と患者窓口の設置

医療関係事業者は、個人情報の適正な取り扱いを推進し、漏洩等の問題に対処する体制を整備する必要がある。このため、個人情報の取り扱いに対し、専門性と指導性を有し、事業者の全体を統括する組織体制・責任体制を構築し、規則の策定や安全管理措置の計画立案等を効果的に実施できる体制を構築するものとする。

出典：医療・介護関係事業者における個人情報の適切な取り扱いのためのガイドライン

2｜就業規則(服務規程)や労働契約書への明記

個人情報保護に関し、「モラルの向上を」といいますが、これだけ情報にあふれている現状において、実際に何をどうしたら良いかまで具体的に指示指導しなければ、スタッフに浸透しません。何故個人情報保護をしなければいけないのかという目的と、どうしなければいけないか、といった項目の具体化が必要です。

(1)就業規則(服務規程)の事例

■服務規程（遵守事項）

●第〇〇条　従業員は、以下の事項を守らなければならない。

①許可なく職務以外の目的で医院の施設、物品等を使用しないこと。

②職務に関連して自己の利益を図り、又は他より不当に金品を借用し、若しくは贈与を受ける等不正な行為を行わないこと。

③勤務中は職務に専念し、正当な理由なく勤務場所を離れないこと。

④医院の名誉や信用を損なう行為をしないこと。

⑤在職中及び退職後においても、業務上知り得た医院、取引先、患者等の機密を漏洩しないこと。(医療従事者の守秘義務として雇用終了後も守ること)

⑥許可なく他の医院等の業務に従事しないこと。

⑦酒気を帯びて就業しないこと。

⑧勤務中は携帯電話等の持ち込みはしないこと。

⑨医院で知りえた情報や医院内であった事、不平不満等をツイッター、ブログ、フェイスブック等に掲載しないこと。(医院の評判を落とす行為も禁止)また、ライン等により他人に知らしめる行為をしないこと。

⑩その他従業員としてふさわしくない行為をしないこと。

(2)労働契約書に記載する解雇規定等

■解雇規定

●解雇規定

(1) 職員が次のいずれかに該当するときは、３０日前に予告をするか、又は平均賃金の３０日分を支払って解雇する。

①職員が精神又は身体の障害により、業務に耐えられないと認められる場合

②職員の勤務能力が著しく低下した場合

③職員の勤務成績又は業務能率が著しく不良、その他職員として不都合な行為があった場合

④事業の縮小その他事業の運営上やむを得ない事情により、職員の減員等が必要となった場合
⑤医院の承認なしに他に就職し、または自己の業務を営むに至ったとき
⑥出勤状態不良のとき、または無届欠勤のある場合
⑦その医療機関内で知りえた情報（医療機関、患者、患者関係者に関する一切の情報）を漏らしたとき。（守秘義務は退職後も反映される）
院内であったこと、不平不満等をフェイスブック、ツイッター、ブログ等に掲載したとき
⑧前各号に準ずるやむを得ない事由があるとき。

3｜情報漏洩したスタッフへの対処

スタッフがブログやツイッターなどで、医院の社会的信用が失われる書き込みが発覚したら当然に解雇理由になります。

裁判所では、能力不足や協調性不足については、医院に対して比較的厳しい見方をしますが、対外的に影響のあるネット上での問題に関しては、多大な影響を及ぼすと考え、解雇へのハードルは緩いといえるようです。誰でも言ってしまうような愚痴やボヤキでは単なる注意をとされるようですが、特定した患者さんや院内の事情が含まれているものであれば、厳しく対処できるようです。ただし、注意しなければいけないのは、この事情で裁判となると患者さんの証言などが要求される場合があります。

(1)指導と改善

情報漏洩が発覚した後、「指導して、改善に機会を与える」ことが重要です。いきなり解雇は、その内容の重要度が相当高い必要があります。逆に内容の重要度が低くても、改善のチャンスを何回与えたかによって解雇と出来ることがあります。

(2)話し合いによる解決：退職勧奨

問題スタッフに退職して欲しい時には、誠意をもって、話し合いによる退職勧奨で解決を目指すことが基本です。話し合いで合意に至れば、お互いの感情的なしこりが少々あってもスムーズに退職となります。解雇であれば不当解雇ということで問題化することも有ります。退職勧奨に関しては、退職に至る理由や当人が置かれている状況、雇用契約や就業規則（服務規程）にどのような記載となっているか等、事前準備が必要です。

■退職勧奨のチェックポイント

●言動や行動に、契約内容に反するような行為があったか。
●言動や行動に、就業規則の解雇などの条文に該当する行為はあったか。
●入職時に契約内容を確認していたか。それを証明できる書類はあるか。
●就業規則を、周知していたか。スタッフが閲覧可能であったか。

問題スタッフへの退職勧奨は、過去に注意や指導をどれだけ行ってきたか、という経過と就業規則や労働契約書に退職勧奨の基準が明記されていることがスムーズに進むポイントです。

退職勧奨は、あくまでも話し合いであって、一方的な通達ではないこと、相手側が行ったことをなじる場でないことを認識し、望まなければいけません。

4｜個人情報漏洩保険への加入

各保険会社では、個人情報漏えい事故に対し、保険を整備しています。業務過誤賠償責任保険普通保険約款、個人情報漏洩特約、危機管理コンサルティング費用特約、危機管理実行費用特約などを付加し、個人情報が漏えいした場合の賠償リスクを補償しています。

■保険対象

【賠償責任部分】
●法律上の損害賠償金
●賠償責任に関する訴訟費用・弁護士費用などの争訟費用
●求償権の保全・行使等の損害防止軽減費用
●事故発生時の緊急措置費用

【費用損害部分】
●謝罪広告掲載費用・会見費用
●御詫び状作成・送付費用
●見舞金・見舞い品購入費用（被害者 1 名に対し上限が設定）
●コンサルティング費用（1 事故あたりの上限が設定）
●コールセンター委託費用等

歯科経営情報レポート　12月号

情報漏洩はトータルな対策が重要　歯科医院の個人情報漏洩対策

【著　　者】中央税務会計事務所
【発 行 者】中島　智
【発　　行】中央税務会計事務所
さいたま市中央区大戸 6-30-1
TEL：048-855-4466　FAX：048-855-2288