８．個人情報に関する事故（漏えい・き損等）発生の場面

本節では、個人情報に関する漏えい、き損等の事故発生時に迅速且つ適切に対応するための方策や、顧客に対して適切に対応を行うための取組などを取り上げている。

（事故発生に備えた取組・対策）

例えば、セキュリティ事故発生時には担当役員の携帯電話に 24 時間 365 日必ず電子メールが自動送信されるような仕組を構築している事例（①）などについて紹介しているほか、委託元との連携まで含めて事故発生時に必要な対応方法を定めている事例（⑤）も紹介している他、事故発生時には混乱が生じることを見越して、報告を段階的に分け、必要な情報だけを先に、正確に入手できるように工夫している事例（⑥）もみられる。さらには、事件・事故の発生報告から対応結果までの情報集約を自動化・一元化しているような事例（⑧）もみられる。

（事故発生後の取組・対応）

例えば、顧客への迅速な連絡に努める場合には、郵便やメール、電話などを順次利用して確実に顧客への連絡を実現した事例（⑨）もあるし、逆に混乱回避のために社内での確実な原因究明・対策実施を優先した事例（⑩、⑰）も紹介している。また、コールセンターでの対応実態・事例（⑯、㉒）も紹介している。

加えて、顧客からの信頼維持・回復のために、個別に顧客（法人）に応じた説明資料を作成して営業担当が説明に回った事例（⑬）や、顧客（消費者）の声を聞くためのアンケートや掲示板を設置したような事例（⑳）も紹介している。

さらに、事故発生時に発生する膨大な作業量に対応するため、専門家等外部リソースを有効活用した事例（⑭、⑱）も紹介している。

また、情報の錯綜や風評被害を防止するためのユニークな取り組みとしては、積極的に大手メディアに情報提供を行い、より正確な報道がなされるようにした事例（⑲）も紹介している。

本節で紹介している取組事例

8-①：**セキュリティ事故が発生した際には、発生日時を問わず（24 時間 365 日対応）担当役員の携帯電話に事故発生の通報電子メールが転送され、迅速・適切な対応を可能としている**

8-②：**個人情報漏えい事故対策訓練を実施**

8-③: **ファイル共有ソフトでの情報流出時には個人情報の含まれるファイルの検索を専門家に委託し、“専門家でも特定しづらくなった”ことをもって顧客を説得**

8-④：事故発生時の対応規程があり、対応フローが定まっている
8-⑤：委託元と連携した対応体制の整備
8-⑥：事故発生時の混乱や不要な報告を防ぐため、漏えい発生時の報告は 2 段階に分け、第一報では必要な最低限の情報を挙げてもらうようにしている
8-⑦：PDCAは現場でまわし、現場から役員に事故詳細と解決策を報告させる
8-⑧：事件・事故の発生報告から対応結果までの管理と重大な事件・事故の報告を自動化
8-⑨：郵送、メール、電話の順に連絡手段を使い分けて全顧客へ、いち早く連絡することを優先
8-⑩：顧客からの問い合わせの蓄積により、顧客の知りたいこと、顧客に伝えるべきことを整理し、的確な対応を実現
8-⑪：ASPサービスを利用している場合でも、バージョンやカスタマイズ状況によっては自社が利用しているASPのみ脆弱性に問題があることがあるので確認が必要
8-⑫：外部委託先の独自調査だけでなく、コストはかかっても、専門性の高い企業に漏えいの可能性についてのセカンド・オピニオンを求めることが有効
8-⑬：原因究明に迅速に着手し、顧客・警察・監督官庁へ連絡
8-⑭：事故後 1 ヶ月間、役員が交代でコールセンターを深夜まで運営
8-⑮：顧客対応として、「迅速なお知らせ」よりも「適切な状況把握」と「対応策の実施」を優先することで、混乱と二次被害の発生を防止
8-⑯：外部リソースの有効活用により、迅速で適切な対応を実現
8-⑰：過大な報道による風評被害・混乱を防止するため、敢えて大手新聞社に事故情報を詳細に説明して正確な情報を報道してもらう
8-⑱：事故後、顧客の声を聞くためのアンケートや掲示板等の設置で信頼回復に尽力
8-⑲：公表と再発防止策の徹底
8-⑳：コールセンターを立ち上げ、問合せ・苦情に対応

※⑨以降の事例は、実際に事故に遭った事業者に対し、事故発生の経緯や、事故後の顧客対応、採用した改善策などを詳細に確認したものである。

8-①【セキュリティ事故が発生した際には、発生日時を問わず（24 時間 365 日対応）担当役員の携帯電話に事故発生の通報電子メールが転送され、迅速・適切な対応を可能としている】（情報サービス業：約 6,700 人）

・L 社では情報セキュリティ事故発生の場合に誰が何をするか、マニュアルを用意している。

・いち早く正確な事故情報を把握することに重点を置いている。

8-②【個人情報漏えい事故対策訓練を実施】

（情報サービス業（ソフトウェア）：約 2,000 人）

・M 社では平成 18 年 11 月に漏えい事故を想定した訓練を実施。個人情報漏えい事故の発生を想定し、緊急対策本部を設置し、顧客からの問合せ窓口や営業対応、報道対応などを訓練する。訓練は事前に各部署に連絡し、協力を得る。

・事故時の対応については規程で決まっている。事故が発生することは望ましくはないが、いざという時に社内的な混乱を起こさないようにしたい。

8-③【ファイル共有ソフトでの情報流出時には個人情報の含まれるファイルの検索を専門家に委託し、“専門家でも特定しづらくなった”ことをもって顧客を説得】

（その他サービス業（教育、学習支援）：約 1,200 人）

・S 社ではファイル共有ソフト（Winny 等）で情報流出事故があった際には該当するすべての方にお詫びの手紙を送った。

・ファイル共有ソフトに関して 1 ヶ月間、監視を専門家に依頼して行った。監視を続けるにつれて個人情報を含むファイルの検索時間が延びていったので、それを報告した。

・『検索によって個人情報が発見される可能性が完全に無くなった』ということは言えないため、検索時間が相当程度長時間化し、当該ファイルが専門家でさえもネットワーク上で特定することが容易ではなくなったことを示し、リスクが相当程度縮減したことを説明することで、顧客の納得を得ることができた。

・事故発生時の対応、情報伝達手順は定まっている。事故後の対処はマニュアル等の原則に従いつつもケース・バイ・ケースである。

8-④【事故発生時の対応規程があり、対応フローが定まっている】（卸売業：約 1,500 人）

・ウ社では、事故の発生に際しては、「インシデント対応規程」があり、緊急時の対応フローが定まっており、上長への報告、事務局への報告、対策委員会の発足などの体制ができている。情報セキュリティやリコールなど様々なインシデントに対応できるようなフロー構築ができており、召集するメンバーは場合によって異なる。

・事故発生の際は、事故発生報告書を管理者が提出する。事故発生報告書は文章で、5W1H を明確に記入することで、時間をかけず分かりやすく書けるよう工夫されている。

8-⑤【委託元と連携した対応体制の整備】

（情報サービス業(アウトソーシング等)：約 1,400 人）

・ク社では、事故発生時の報告体制について、委託元と連携した対応体制を整備している。

・委託元とは、委託元が主催する「合同リスク検討会」に毎月出席し、事故や問い合わせに対する状況を報告し、今後の対応などについて検討している。

8-⑥【事故発生時の混乱や不要な報告を防ぐため、漏えい発生時の報告は 2 段階に分け、第一報では必要な最低限の情報を挙げてもらうようにしている】

（その他サービス業(印刷・広告)：約 1,400 人）

・コ社では、事故などが起きたときに備えて緊急連絡表を設けている。慌てると何を報告してよいかがわからなくなるので、第一報ではどの程度の内容を報告し、第二報以降ではどの程度報告するのか、という点で 2 つの段階に分けて報告するようにしている。第一報用のフォーマットを作成している。

・そのように、「どこまで報告するか」ということを明確にしていないと、何度も電話で現場の担当者に聞きなおしたりする手間が生じた事例があったからである。不要な情報ばかり報告され、本当に必要な情報の報告が遅れることを懸念していることによる対応である。

・漏えいなどの事故が生じた場合に備え、「公表判断基準」を策定している。「管理主体は誰か」「漏えい形態はどうか」「漏えい内容はどうか」「漏えい情報量」「被害の大きさ」の 5 つの視点で判断し、公表するか、公表しないか、ということを明確にしている。公表に際しては経営企画部とも連携している。

8-⑦【PDCA は現場でまわし、現場から役員に事故詳細と解決策を報告させる】

（製造業：約 26,000 人）

・サ社では事故が発生した際は、定型フォーマットで再発防止策を現場から全社事務局に提出させている。全社事務局が添削したものを、現場で再検討のうえ、全社事務局を通じて経営会議内に報告している。

・なお、漏洩事故については、高度な暗号化による秘匿化や秘密分散による情報分散化、遠隔操作による内蔵データの消去といった安全管理対策を講じた場合であっても、現場からの反発（技術的措置を採用しても事故の報告対象になるならば当該措置の開発や採用のインセンティブが失われる）を制して、報告対象としている。

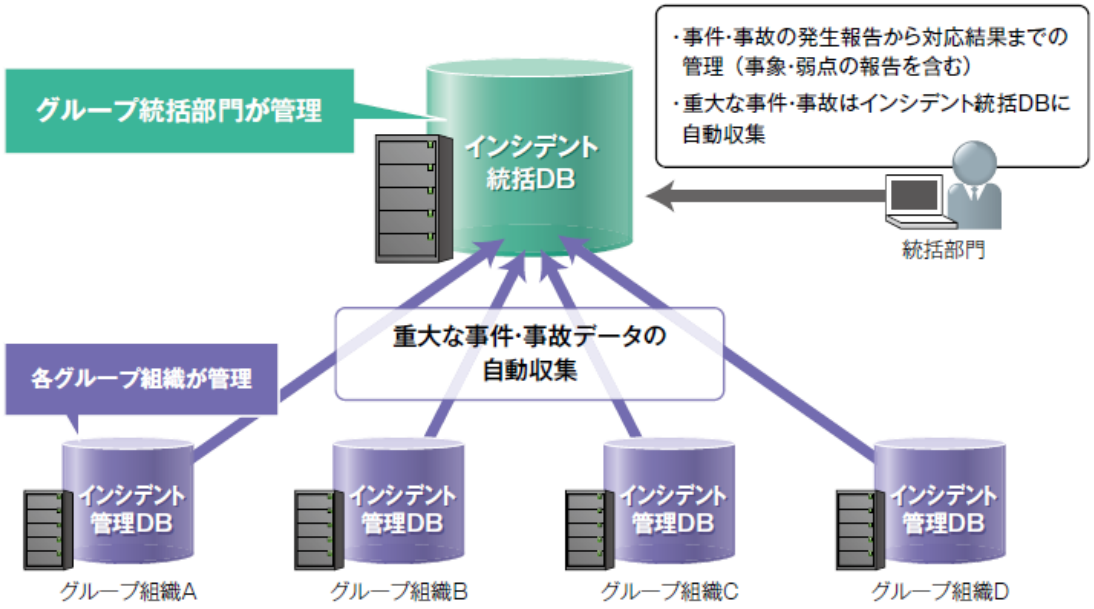
8-⑧【事件・事故の発生報告から対応結果までの管理と重大な事件・事故の報告を自動化】（製造業：約 12,000 人）

・シ社では以下のように事件・事故を管理している。

インシデント管理データベース：　グループ各組織は、事件・事故の発生報告から対応結果までの管理と、事象・弱点を報告できるツール「インシデント管理データベース」を使い、事件・事故情報を共有している。また、報告者に対策実施期限を自動で知らせるエージェント機能を付加するなど各種の工夫を加えている。これにより事件・事故対応の迅速化、情報の共有化、各組織でのツール維持のための負荷軽減などの利点がある。機微情報が入っていることから、各管理データベースは各部門の管理データベース担当者とその上席者（報告ライン）と、各組織の ISMS 担当者のみしか閲覧できない。

インシデント統括データベース：　グループ各組織のインシデント管理データベースに報告された事件・事故のうち、特に重要な事件・事故については、リアルタイムにインシデント統括データベースに反映される。重要な事件・事故は、例えば「社外秘以上の情報を格納した USB メモリ、パソコンなど電子媒体の紛失・盗難事件・事故」のように定義されている。グループ統括部門は、重大な事件・事故に対して、原因分析と暫定対策、恒久的な再発防止策、予防策を検討し、グループ各組織にフィードバックしている。

図表　インシデント管理 DB によってグループ全組織の事件・事故の報告管理方法を統一



8-⑨【郵送、メール、電話の順に連絡手段を使い分けて全顧客へ、いち早く連絡することを優先】（情報サービス業(ソフトウェア)：約 500 人）

・ソ社では事故発生を認識した当時は、誰が何をしたら良いか全く分かっていなかったことから、“エンドユーザーも含む利害関係者に説明を行うこと”を最優先することにした。この判断は社長によるトップダウンの判断であった。
・告知文の作成と連絡対象者のリストの作成後に全ての顧客向けに書簡を送付し、記者会見を実施。翌日には新聞 5 紙に漏えい事件発生についての謝罪広告を掲載した。
・全顧客に書簡で、個人情報の漏洩の可能性を伝える書簡を郵送した。数%は宛先不明で書簡が戻ってきた。特にオンラインで商品をダウンロードして購入した顧客に連絡をつけるのが難しかった。理由はダウンロード購入の場合、商品の発送が伴わないため、登録された住所に不備が多かったことによる。住所不明の顧客には、同じ内容のメールを送付した（メールアドレスは確実に把握していた)。それでもメールが戻ってきた場合は、電話番号がわかるときには電話をした。残り数百名分はどうしても連絡がつかず、ホームページへの掲載などで対応した。

8-⑩【顧客からの問い合わせの蓄積により、顧客の知りたいこと、顧客に伝えるべきことを整理し、的確な対応を実現】（情報サービス業(ソフトウェア)：約 500 人）

・ソ社では当初はいち早く漏えいの発生を顧客へ伝達することを優先したため、コールセンターでの想定問答などの検討・作成が十分でなかった。このため、当初の問い合わせには十分に回答することができなかった。顧客への対応は公表前にもう少し検討したほうが良かったようにも思うが、逆に顧客からの直接の問い合わせ内容を聞かないと、何を顧客に伝えなくてはいけないのか、ということについてはわからなかったとも考えている。
・なお、漏えいの状況や原因は十分には解明されず、全て結局は「可能性がある」という調査結果で終わってしまったため、追加で有益な情報提供をすることができなかった。

8-⑪【ASP サービスを利用している場合でも、バージョンやカスタマイズ状況によっては自社が利用している ASP のみ脆弱性に問題がある場合を考慮して確認が必要】（情報サービス業(ソフトウェア)：約 500 人）

・ソ社ではサイトの運営は外部企業に委託を行っていた。ASP による EC サイトの運営、コールセンターでの対応も含めて委託を行っていた（外部委託先企業は EC サイト運営、コールセンター運営も独自の事業として実施していた)。
・なお、この外部委託先の ASP を利用していたのは同社以外に 50 社程度あったが、実際に被害にあったのは同社だけであった。同社の EC サイトのための ASP だけがバージョンが古かったことが原因のようであった。「SQL インジェクションには対応済み」というようたい文句に安心していたが、実際には脆弱性があり、SQL インジェクションを許してしまったようであった。

8-⑫【外部委託先の独自調査だけでなく、コストはかかっても、専門性の高い企業に漏えいの可能性についてのセカンド・オピニオンを求めることが有効】

（情報サービス業(ソフトウェア)：約 500 人）

・ソ社ではクレジットカード会社からの指摘を受け、最初は外部委託先に事故の可能性について調査を依頼した。この結果、「問題がなさそうである」という報告があったので、EC サイトの閉鎖までは考えなかった。このため、事故発生を認識するのが一層遅れてしまった。

・クレジットカード会社からさらに指摘を受け、同社が推薦する調査会社に委託したところ、10 日程度で調査結果が出て、漏えいの可能性のあることが明らかになった。

・その後、関係者の要望に合わせてさらに複数の調査会社に委託して調査をしたが、調査結果は同じになったので、この調査結果が信頼できるということがわかった。

8-⑬【原因究明に迅速に着手し、顧客・警察・監督官庁へ連絡】

（情報サービス業（アウトソーシング等）：約 30 人）

・タ社では出会い系サイトからスパムが送信されているという苦情が、同じ日に多くの顧客から寄せられ、携帯メールアドレスの漏えいの可能性に気づき、警察へ通報、当日夜から調査を開始した。

・最初に、どこのサーバ上のどこの企業の顧客の情報が流出したか調査した。その結果、原因までは分からなかったものの、管理画面に不正アクセスと思われるログが発見された企業があり、同社が事故を起こした可能性が高いことが判明した。

・翌日、同社は顧客と警察に漏洩事故発生の可能性を連絡した。主務官庁等へは先ず顧客が連絡し、その後同社から連絡した。

・二日後、アクセスログ解析結果より、警察の要請に基づき、インターネットプロバイダーに協力してもらい、アクセス元を調査したところ、繁華街のインターネット喫茶から同社のサーバにアクセスされていることが判明し、事故であることを特定した。

・その後、同社ホームページで、漏えい事故が発生したことを公表。顧客企業のユーザーには、顧客企業がそれぞれ連絡した。同社は、顧客企業よりも先に公表できないことから、公表のタイミングを調整する必要があった。

8-⑭【事故後 1 ヶ月間、役員が交代でコールセンターを深夜まで運営】

（情報サービス業（アウトソーシング等）：約 30 人）

・タ社では事件公表から約一ヶ月間、同社内に事故対応のコールセンターを設置し、電話とメールで応対した。

・受付日時は、土日関係なく、朝 10 時～26 時（深夜 2 時）まで。

・体制は、基本的にすべて役員が交代で対応した。社員にはほとんど対応させなかった。

・対応を始めて一ヶ月が経過してからは、コールセンターに委託したが、二次的にエスカレーションさせて同社にも繋がる体制を整えていた。
・顧客企業と調整し、事故に関するユーザーからの連絡はすべて同社で受け付けるようにした。これは、被害にあったユーザーが、たらいまわしされることなく、均質の応対をうけることができるようにするためである。
・スパムを完全に停止させるためには、メールアドレスを変更していただくしか方法はなかったため、ひたすらお詫びを申し上げた。
・クレームの受付は、メールが 1,000 件、電話が 300 件で、メールが圧倒的に多かった。

8-⑮【顧客対応として、「迅速なお知らせ」よりも「適切な状況把握」と「対応策の実施」を優先することで、混乱と二次被害の発生を防止】
（情報サービス業(e コマース)：約 60 人）

・チ社では、顧客の個人情報が漏えいした可能性があることがクレジット会社からの調査依頼により発覚した。結局、数十万人分の情報が漏えいした疑いがあった（うち、クレジットカード情報を含む情報は数万人分)。
・翌日より、まず「対策本部」を設置し、次いで「封じ込め（拡大防止)」を開始し、その後「分析・追跡」に 2 週間程度を要した。その後、対策改善を行い、顧客からの問い合わせ窓口も設置した上で「公表」を行った。
・いち早く顧客に漏えい事故の発生をお伝えすることとのトレードオフで、正確な被害状況把握のために公表まで精査期間を設けたことが、自社でリスクを感じながら採用した方策である。
・社内体制としては、役員と経営戦略室が「方針指導」、「公表」の対応を行い、システム部が「封じ込め」、「分析・追跡」、「対策改善」を担当し、オペレーション部が「窓口設置」を、更に残りの全スタッフも「顧客対応」に協力した。
・結局、公表までタイムラグが 1 ヶ月程度発生したのだが、それは顧客向けコールセンターの設置や原因・現状等を明確にし、公開時に顧客にきちんと説明責任をはたせるようするために時間が必要であったことが理由である。
・顧客からは、なぜ早く公表しなかったのかというご意見をかなり頂戴したが、体制が整わないまま公表していれば、顧客に正しい情報を伝えられずかえって迷惑をかけただろうと思われる。

8-⑯【外部リソースの有効活用により、迅速で適切な対応を実現】
（情報サービス業(e コマース)：約 60 人）

・チ社では問題発覚後、セキュリティ調査会社にすぐに連絡し、対策を相談した。
・社内だけでは対応しきれないと判断し、日常的にサイトの構築などで付き合いのあるシステム会社の社員２名に同社に来てもらい、対応体制を整えた。

・システム上の脆弱性の修正のために、リモートで支援を行う協力会社の 12 名と、同社のシステム担当の 4 名が 3 日間、ほぼ 24 時間体制で対応を行い、脆弱性の修正にこぎつけた。

8-⑰【過大な報道による風評被害・混乱を防止するため、敢えて大手新聞社に事故情報を詳細に説明して正確な情報を報道してもらう】
（情報サービス業(e コマース)：約 60 人）

・チ社では IR や PR も掲載したが、その内容がそのまま顧客や社会に伝わるかは非常に不安であった。そこで、特定の大手新聞社に対して同社から情報を提示し、先に取材してもらって、できるだけ間違いがないように報道してもらえるような工夫を行った。
・当然に新聞社の原稿であるので、掲載前に記事を確認させてもらうことはできなかったのだが、一部は少し過大に書かれた部分もあったものの、間違いが少なく報道してもらうことができた。特定新聞社にリークしたことで、その会社が一番詳細に漏えい事故の情報について報道することができ、結果として他の新聞紙よりも耳目を集め、IR や PR の趣旨を損ねることなく正確な情報を伝えることができた感じている。

8-⑱【事故後、顧客の声を聞くためのアンケートや掲示板等の設置で信頼回復に尽力】
（情報サービス業(E コマース)：約 60 人）

・チ社では事故以降、新たに顧客の声を聞くためにアンケートを設置した。また、Web 上で情報を双方でやり取りできる専用の仕組みを設置した。顧客の声を取り入れながら、個人情報問題やその他 CS についての対応を考えていくようにしたのも 1 つの工夫である。事故当時はお叱りもあったが、励ましの言葉も多数あった。e コマースはお客様によって支えられる事業であることを痛感した。
・アンケートに寄せられた指摘については、必ずしも 1 つ 1 つに回答しているわけではないが、ある程度溜まった段階で、回答レポートのような形でまとめて資料をブログ形式で掲載している。

8-⑲【公表と再発防止策の徹底】（その他サービス業（印刷・広告）：約 10,000 人）

・テ社では事故判明後、個人情報保護に関する危機管理計画に従い、迅速に対策本部を立ち上げた。組織が一体となって対応を進めることが必要である。
・事実関係および再発防止策を速やかに発表できるようにすることが重要であり、そのためには、事故による影響範囲の特定、2 次被害の防止、徹底した原因究明と事故発生をリアルタイムに検知し漏えいさせない対策が必要である。具体的な再発防止策としては、カメラ監視や従業員教育の強化等の一般的対策の他に、個人データ記憶媒体を取り扱う担当者数を極少化して社員に限定、個人データ記憶媒体を取り扱うことのできるエリアを隔離し入退出時の警備員による金属探知検査、複数の企業による外部監

査等を行っている。
・再発防止策をたてると共に、個人情報を取り扱う担当者全員への運用と教育を徹底し、維持継続している。

8-⑳【コールセンターを立ち上げ、問合せ・苦情に対応】
（その他サービス業（印刷・広告）：約 10,000 人）
・テ社ではコールセンターは、情報統制上の観点から、コールセンター業務を行っているグループ会社に設置し、ピーク時は限定した社員による増員で対応した。
・事件発生から二ヵ月ほどでコールセンターへの問合せはほぼ無くなっている。