

在職者による情報漏洩

ケース2
IDF コミュニティ 2007

外部からの通報

2007年12月7日 社外の（善意の）第三者より、社内で管理している顧客情報が外部で売買されているという情報提供があった。

情報提供者の情報をもとに、売買されている顧客情報リストの一部を入手し、内容を確認したところ、偽造などではなく確かに社内サーバーのデータベースに登録されている営業で使用している情報である事が分かった。

このデータは、重要な取引先の共有顧客情報も含むため、会社への被害は甚大になると考えられた。

顧客情報による絞り込み

入手した顧客情報を精査したところ、それらは全て特定の営業部によって登録されたものであり、かつその中の最も新しいものは2ヶ月前の10月3日に登録された情報である事が分かった。

情報漏洩が発生したのは、10月3日以降と判断し、調査が行われる事になった。

アクセス制限

顧客情報が保存されていたデータベースはユーザーID毎にアクセス制限が設定されていた。

データベースへのアクセス制限のグループは数種類存在するが、該当データへのアクセスに関しては、データの閲覧のみ許可されている者と、登録及びデータの出力まで許可されている者が存在した。

調査対象者の選定

サーバーへのアクセスログの解析から、調査対象となった営業部の登録データを出力できる権限を持ち、かつ10月3日以降にデータベースへアクセスした履歴のある者は10名存在する事が判明した。

この10名を重要調査対象者として調査する事になった。



調査方針の決定

直近2ヶ月間に10名のPCから外部へ情報が漏洩した痕跡が存在するか、調査を行う事になった。

初めに10名分のサーバーに保存されているEメールと外部メディアへの情報の持ち出し（セキュリティツールが導入されていた）に関する調査が行われる事になった。



Eメールの調査

社外へのEメール送信に関しても特定の社員に限定されていたが、10名全て送信が許可されていた。

サーバーに保存されているEメールを調査し、10月3日以降における社外へのEメール、添付ファイル付きのEメールを中心に調査を行ったが該当する個人情報が発見されなかった。

外部メディアによる情報持ち出し調査

USBメモリなどの外部メディアの使用に関しては、使用を許可された者にのみ、物理的に使用可能なPCが割り当てられていた。

また、そのPCを使用し外部メディアへファイルがコピーされた場合には、コピーした日時やファイル名がログとして記録されるセキュリティツールが導入されていた。

外部メディアによる情報持ち出し調査

10名全てに外部メディアへの書き込み可能なPCが与えられていた。外部メディアへファイルをコピーした履歴が残っていた者は4名であった。

外部メディアへコピーされたファイル名を調査したが、通常の業務で使用されているファイル名（今回の漏洩情報は含まれない）のみであり、特に疑わしいファイル名は存在しなかった。

端末PCのコンピューターフォレンジック調査

ここまでの調査において有力な手がかりを掴む事はできなかった。

調査対象者10名のより詳細な調査を行う為、10名分全てのPCにおいてコンピューターフォレンジック調査が行われる事になった。



端末PCのコンピューターフォレンジック調査

コンピューターフォレンジック調査の調査ポイントは以下のように設定された。

1. 漏洩したものと同一2007年10月時点での登録情報をPC上に出した痕跡が無い、削除データを含むハードディスク全領域の検索を行う。



端末PCのコンピューターフォレンジック調査

2. 社内のサーバーには保存されておらずWEBメールなどを使用してファイルが送付された痕跡を調査する。
3. 外部メディアへファイルをコピーした履歴の存在するPCに対しては、コピーされたオリジナルファイル内容の調査を行う。
(ログに記録されているのはファイル名のみであり、簡単に偽装、変更が可能であり、実データは問題となっている情報である可能性がある。)

端末PCのコンピューターフォレンジック調査

情報システム部門の協力により、調査対象者10名が使用しているPCの証拠保全が行われた。

コンピュータフォレンジック調査の結果、該当する顧客情報は全てのPC内において検出されなかった。また、WEBメールなどの不正使用の痕跡も無く、外部へコピーされたファイルも顧客情報を含まない通常の業務で使用されるものであった。

出勤記録の調査

データをコピーできる権限者以外の漏洩経路を確認するため、調査対象者10名の出勤記録、PCの稼働状況とデータベースへのアクセス履歴の照合を行ったところ、10名のうちの1人であるA氏が退社後と考えられる時間に、A氏のユーザーIDでデータベースへアクセスされている事が新たに判明した。



出勤記録の調査

A氏のユーザーIDによって、データベースにアクセスされた時間帯に、同じ部署内には5名の社員がいた事が入退出記録から分かった。

この5名にはデータベースへアクセスする権限は無く、また社外へのEメール送信や外部メディアの使用も許可されていない社員であった。

5名の中にはA氏の部下であるB氏も含まれていた。

端末PCのコンピューターフォレンジック調査

この5名のうちのだれかがA氏のID/パスワードを不正に入手し、データベースへアクセスした可能性があるかと判断し、追加で5台のPCのコンピューターフォレンジック調査を行う事になった。

端末PCのコンピューターフォレンジック調査

コンピュータフォレンジック調査を実施したところ、A氏の部下であるB氏のハードディスク内において、漏洩したものと同一2007年10月3日時点の登録情報を含む顧客情報が削除ファイルとして検出された。

他の4名のPCからは一切検出されなかった。



端末PCのコンピューターフォレンジック調査

B氏のPCを更に調査していったところ、WEB上に大容量のデータを保存可能なストレージサービスサイトにアカウントを作成し、顧客情報リストをアップロードしている事実が判明した。

インターネットの使用に関しては全的にWEBフィルターを採用していたが、ストレージサービス系のサイトへのアクセスは制限されていなかった。

本人へのインタビュー

コンピューターフォレンジック調査により決定的な証拠を得る事ができた為、B氏本人へのインタビューを行った。

B氏は顧客情報リストをストレージサービスサイトを経由し個人PCにダウンロードした事を認めた。動機は顧客情報リストを売却する事によって得る金銭目的であった。

本人へのインタビュー

A氏のID/パスワードを知っていた理由としては、A氏が手帳の中にID/パスワードをメモしている事を知っていて、A氏が席を外している間に盗み見たという事であった。

その後、B氏は自宅謹慎を経て、最終的には懲戒免職となった。

A氏もパスワードの管理責任を問われて、訓告処分を受けた。