1-1　個人情報の流出
ネットワークや職場のずさんな管理が原因

「個人情報」とは、氏名、生年月日、住所、電話番号など、その情報単体、または他の情報と照合することで、特定の個人を識別できる情報のことをいいます。

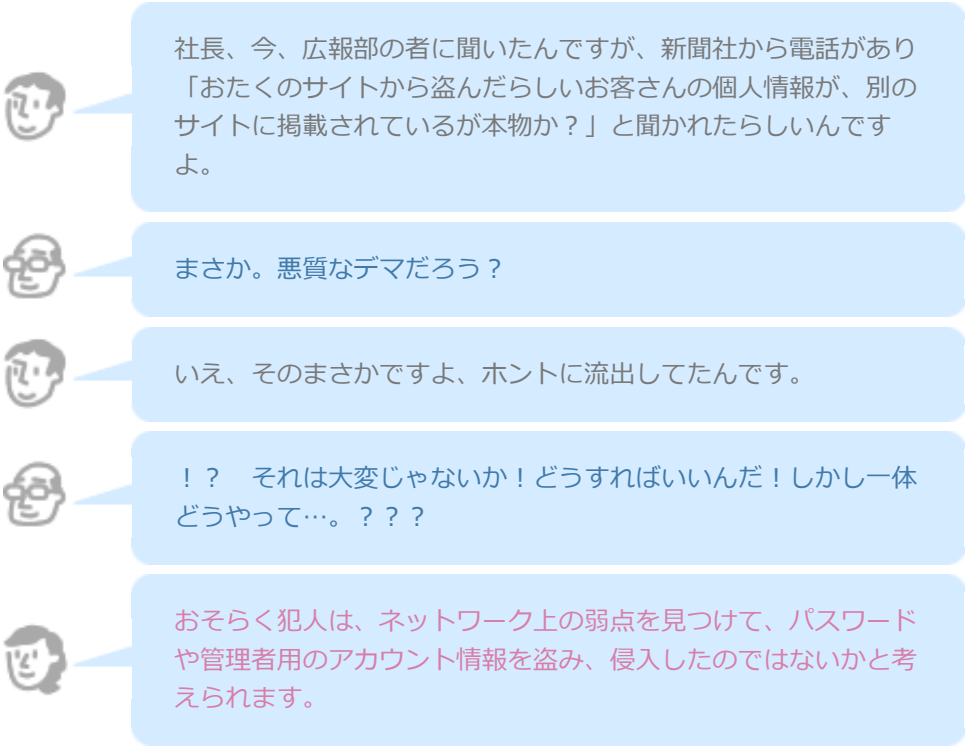
個人情報が盗まれた場合、どうなるのでしょうか。またその目的は何でしょうか。大きく分けると次の２通りが考えられます。

１．金銭目的
　名簿業者等に持ち込み売買され、DMの発送や商品の購入、サービスの勧誘等に利用される。
２．恨み・嫌がらせ
　企業に対して、不満・恨みを持っている、あるいはネットマニアが嫌がらせのために情報を盗み、その内容をネット上等で公開する。

盗難以外では、従業員が社用PC・スマートデバイスや資料を、外出先で紛失するケースがしばしば起きています。また、会社で許可されていないファイル交換ソフト、クラウドサービスを利用していて、本人の意思とは無関係に個人情報や機密情報が、ネットワーク上に流出してしまうこともあります。

あの時ちゃんとセキュリティできてたら…

～ダメダメコーポレーションの場合～



では、この「ダメダメコーポレーション」は、なぜ外部者に情報を盗まれたり、侵入されたりしたのでしょうか。この企業では、次の２つのずさんな管理が原因でした。

→システム担当者やサーバ管理者等の意識の低さ、設定の甘さ

管理者用パスワードが安易な設定であり、かつ、不正な侵入によりパスワードを盗まれないためのシステム側の設定を怠っていた。よって社内に設置されたファイアウォールも無意味であった。

→セキュリティに配慮されていない社内環境、物理的セキュリティの甘さ

サーバを管理・運営するシステム管理室は、鍵もなく人の入退室が自由、その履歴も残していなかった。また、企業への入口（ビルの入口）も同様に管理が不十分であった。データや情報が盗まれる可能性は大いにあった。

ポイント!!

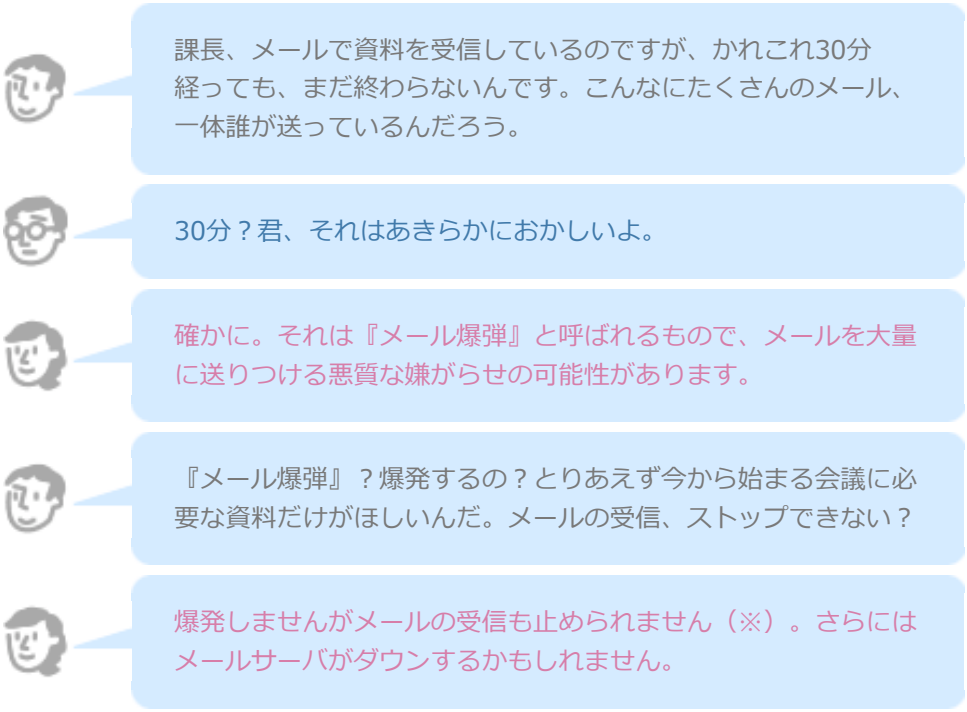
情報漏えいが起きた場合、企業は顧客・消費者からの信頼を失います。そして企業は予想以上の社会的ダメージを被るとともに、企業の存続にも大きな影響を受けることになります。
そのような事態を回避するためにも、ネットワークと現場の環境整備、すなわち物理的セキュリティへの徹底した管理は、取り組みの第一歩となります。

1-2　メールサーバへの攻撃
企業全体の業務をストップさせてしまう『メール爆弾』

電子メールは、今では電話やFAX以上に多用される通信手段です。その機能が麻痺した場合、業務にかなりの支障をきたすことが予想されます。それを逆手にとった悪質な嫌がらせが『メール爆弾』です。同じユーザーに膨大な量のメールを送りつけ様々な被害を与えます。

あの時ちゃんとセキュリティできてたら…

～ダメダメコーポレーションの場合～



「ダメダメコーポレーション」は、結局、この『メール爆弾』により次のような被害を受け業務に影響が出てしまいました。

- ✕ メールボックスの容量が一杯になりその他のメールが受信できなかった。
- ✕ 加入しているインターネットサービスプロバイダのメールサーバがダウンし、別の利用者（企業や個人）にも被害を及ぼした。

受信しなければいいんじゃないか…と思うところですが、残念ながら受信しなければ『メール爆弾』かどうか判断できません。しかも、専用プログラムが開発され送信元が偽装できるため、未然に防ぐのは難しいといえます。

※専門知識をもつ技術者が設定変更等の対策をしメール受信を止めることは可能で

す。

ポイント!!

基本的な対策
（１）受信可能な容量制限をメールサーバで設定する
（２）メールアドレスをむやみに人に教えない

1-3　ウイルスの誤発信

一度感染すると、本人の意志とは無関係に大きな被害を引き起こす。それが、ウイルス。

ウイルスの特徴

・メールの送受信により感染が拡大する
・人間の意思とは無関係にメールとともに勝手に送られる
・メール以外にも、USB等のメディア類やSNSのリンク先不正サイト等の利用によりネットワーク経由で感染する
・コンピュータに誤作動を引き起こしたり使えなくさせる
・クライアントPCやサーバを乗っ取り、遠隔操作される
・IDやパスワードを盗まれ、社内の他のクライアントPCやサーバに伝染する
・常に新しいウイルスが作られている

【ウイルス感染の兆候を見逃すな！】

PCの調子が悪いのは、ウイルスに感染しているから？裏で、ウイルスチェックソフトが仕事をしている場合もありますが、変だなと思ったら、システム管理者にたずねてみましょう。

１）PCの起動に時間がかかるようになった、または起動できなくなった
２）システムの動作が遅くなった、または途中で動かなくなった
３）画面上に、奇妙なメッセージが表示された、または音がなった
４）突然データが消えた
５）身に覚えのないメールを送信している、パソコンの動作が遅い

【主な感染経路には気をつけましょう】

１）メールによる感染（添付ファイル等）
２）ウェブによる感染（ブラウザやファイルダウンロード）
３）ファイル共有ソフト（ファイル）
４）USBメモリによる感染（メモリ自体やファイル）
５）その他のメディア（DVD、CD、スマートフォン等）

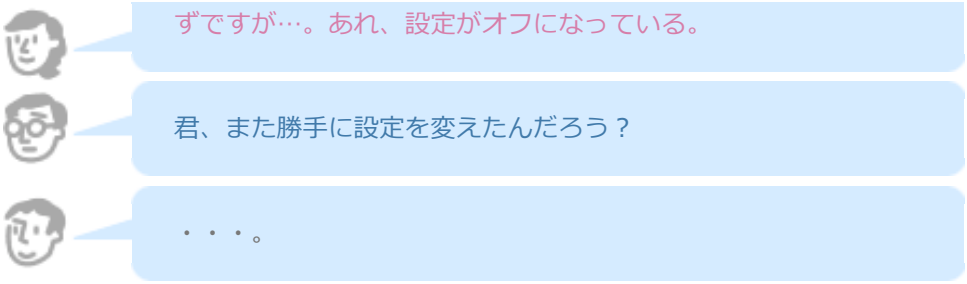
あの時ちゃんとセキュリティできてたら…

～ダメダメコーポレーションの場合～

課長、今取引先から電話があり、僕がメールで送った添付ファイルがウイルスに感染していた、どうしてくれるんだ、と言われたんです。

え？ウイルス？　君、ちょっと見てくれないか。

・・・パソコンがウイルスに感染しているようですね。しかしこのパソコンにはウイルス検知ソフトがインストールされているは



「ダメダメコーポレーション」の失敗

- ウイルス検知ソフトをインストールしていたにもかかわらず、その設定を従業員が勝手に変更してしまい、未然にウイルスを防ぐことができなかった。
- 社外の取引先にまでウイルス感染の被害が広がってしまった。

インターネットのメリットは、世界中どこからでもアクセスできるということですが、そこには、同時に大きな危険性をはらんでいることを覚えておきましょう。

ポイント!!

ウイルス検知ソフトを利用してメールを開く前に対策することが、最も基本的な対処策だといえます。またウイルスの危険性を、従業員に十分周知・教育することも必要です。

1-4　外部からの不正アクセス
ウイルス同様、被害が後を絶たない不正アクセス

ハッカーやクラッカー等による不正アクセスの方法も様々で、代表的な手口として次の６つがあります。

１．システムやサービスを停止させる
コンピュータ通信の仕組み上の弱点を狙った攻撃で、サーバーやクライアントが正常に動作しない、または停止することもあります。業務上受ける影響はかなり大きいと言えます。

２．システムを誤作動させ、重要情報を盗む
サーバーの中にあるパスワードファイルを表示し、システムに誤作動を起こさせたり情報を盗むといった攻撃です。盗まれる原因は、システムの設定に不備があったり、セキュリティ上必要なバージョンアップを怠るなど、管理者側の不備によるところが大きいと言えます。

３．システムの管理者権限を奪う
コンピュータシステム全体を管理するソフトウェア（OS）のバグ（コンピュータプログラムに含まれる誤りや不具合）を利用し、管理者以外の何者かが管理者権限を得る攻撃です。管理者権限を取られてしまうと、次から次へと社内のコンピュータに侵入され、大きな被害につながる恐れがあります。

４．ネットワーク回線の盗聴
社内のネットワーク回線を流れるTCP/IPパケットは、それを監視するプログラムや盗聴用のプログラムで簡単に見ることができます。盗聴プログラムを入れたパソコンを使用すれば、社内のネットワークを流れる電子メール等はいとも簡単に盗聴されてしまいます。

５．パスワード解析
暗号化して管理されているパスワードファイルですが、それらを解析するプログラムが出回っています。とくに、固有名詞等短い単語を使ったパスワードは、解析プログラムによって見つけられてしまう可能性が高く危険です。

６．侵入口となりうる窓口を探す「ポートスキャン」
インターネット上で公開されているサーバコンピュータは「ポート」と呼ばれる接続窓口を複数用意し、利用者からの接続を待っています。「ポートスキャン」とは、このポートに順番にアクセスし、侵入口となりうる脆弱なポートがないかどうか調べる行為です。ポートスキャンすること自体がシス

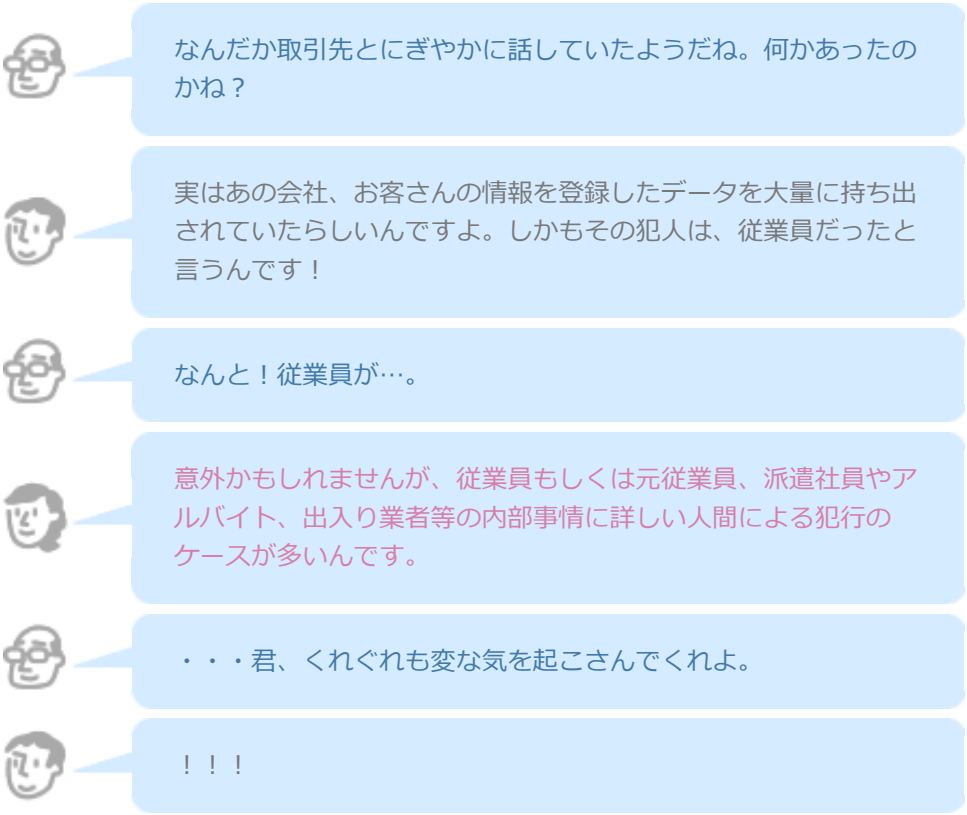
テムに被害を与えることはありませんが、不正アクセスへの準備段階として利用されています。また、ファイアウォールがある場合もしっかり設定されていないと意味がないので注意しましょう。

1-5　内部者による個人情報の不正売買
情報漏えい事件の多くは内部者による犯行

個人情報（顧客情報）は、企業にとってまさに手に入れたい貴重な情報です。悪質な業者もそれらを入手しようと躍起になっています。しっかり管理されていない情報は、外部からの不正アクセスにより盗まれることも十分考えられます。しかし漏えい事件の多くは、実は内部者（従業員、元従業員等）による犯行なのです。

あの時ちゃんとセキュリティできてたら…

～ダメダメコーポレーションの場合～



この「ダメダメコーポレーション」の取引先では、なぜ顧客情報が従業員によって持ち出されてしまったのでしょうか。予測できる原因を３つあげてみました。

→セキュリティに配慮されていない社内環境、物理的セキュリティの甘さ
企業や部署の入口で、受付がない等入退室の管理が不十分、さらにデータや資料等を持ち出せる環境に問題があった。

→情報セキュリティに関する従業員への周知・教育が不十分
情報というものが、金銭と同様に企業にとって重要な資産であると同時に、情報を持ち出す、売買する等の行為は犯罪であることを、従業員に周知・教育する必要がある。

→情報化社会の多くのメリットの反面、デメリットとして犯罪に加担している

コンピュータが普及する以前と比較し、現在では膨大な量の情報もデジタル化されて持ち運びやすくなっている。

ポイント!!

外部からの不正アクセス以外にも内部の不正に対する防御措置を行うことが重要です。大切なのは「個人情報を保護する、一人ひとりのモラル」であると言えるでしょう。