企業はいかにして情報漏洩を防ぐか

～ネットワークを介しての情報漏洩の危険性～

管理行政学科　４年
0050107　　太田　雅文

目次

第１章 情報化社会における企業と情報漏洩の現状

近年インターネットを介した個人情報の漏洩が問題となっている。具体的には企業の顧客データの流出が相次いでおきたり、官公庁の HP 改ざんが多発したりと言ったようなことが問題視されている。こういうことが起きる中で自分達は日々様々な情報流出の脅威にさらされていきている。そこでこれらがいかにして起きるか、またどのようにしたら防ぐ事ができるのかを企業の視点から考えてみたい。

現在、インターネットはビジネスに顕著な影響を与えている。今までの情報化投資が人手による作業の効率化に重点的に活用されてきたが、サービスレベルの向上やスピード競争など経営戦略的なところで本格的に活用されるようになってきた。情報技術がビジネスに与える影響、すなわち広域、大量の情報がやり取りされることで、ビジネスのスピードが上がることや、個々の情報への的確な対応が必要になってきた。企業はビジネスを円滑、効率的に運営する上で、もはやネットワーク技術の存在は欠かせない。ネットワーク技術の重要性は高まるばかりだが、その一方で企業の情報システムに対する不正アクセスの件数も急激な勢いで増加している。企業が不正アクセスによって被害を受けた場合、データやシステムの破壊、情報漏洩などの実害もさることながら、被害者である企業自体が社会的信用を失ってしまい取り返しのつかない状況に陥る可能性もある。このように深刻化する不正アクセスの被害に対応するために、2000 年 2 月にハッキング等の不正アクセス行為を取り締まる「不正アクセス禁止法」が施行された。しかし不正アクセスの報告は後を絶たないでいる。

またウイルス被害や情報漏洩事件が報じられるたびに強調されるものとして企業におけるセキュリティ教育の重要性がある。情報セキュリティに関する損失から企業を守るには、技術的な対策だけでは不十分である。そこでまず企業におけるセキュリティ教育の現状を見てみたい。

まず一般ユーザー向けのセキュリティ教育について考えたい。以前だと講師を招いてセキュリティに関する講義を実施する方法もあったが、社員数が多い企業では大掛かりになってしまう。また収容人員が多い場所を確保しても一度には実施できないという点から、数回に分ける必要があるだろう。そうなると、講師を複数名用意する必要がある。中小規模の企業では, 一度に実施できるとしてもコストの面から実施するのはなかなか容易ではないと言える。また、社員としても業務で忙しい中スケジュールを合わせて講演会場まで出向かなくてはならない。そういう事を考えると効率が悪いのが実情と言える。そのため近年Ｗｅｂを利用したオンライン教育、いわゆるＷＢＴ（Web Based Training）を利用する企業が増えてきている。

次にプロフェッショナルと経営陣向けの教育を考えたい。現場では, 業務で情報セキュリティに携わる人材の教育にも苦労している。一口に“業務で情報セキュリティに携わる人材”といってもさまざまで挙げられる。例えば、セキュリティコンサルタント、セキュ

リティシステムを構築する SE、セキュリティ製品の開発者などが挙げられる。業務の内容によって必要な知識は異なるため一般ユーザー向けのセキュリティ教育のように WBT で教育を受けさせるわけにはいかない。例えば、セキュリティコンサルタントにはセキュリティ・マネジメントの知識は不可欠だが、セキュリティ製品の開発者にはあまり必要ない。その代わり、セキュリティ技術に関する知識が要求される。現在はセキュリティに関する公的な資格として「情報セキュリティアドミニストレータ」があるが、これを取得するための学習はセキュリティに携わる人材の教育手段にはなりにくい。それは情報セキュリティアドミニストレータとは、主に情報システムのユーザーを対象とした資格だからである。そこでセキュリティに携わる人材の教育になるような資格が今後求められている。

そこで２章ではインターネットの発達によって起き始めたネットワークを介する情報漏洩や、企業の内部からの情報漏洩の現状を取り上げていきたい。

また３章では情報セキュリティとはまた企業はどのようにしたら情報漏洩を防げるのか技術的な分野だけでなく、企業内でできる対策について考えていきたい。

そして４章では企業が現状でできうる対策について現状分析とともに考えていきたい。

第２章 ネットワークを介した情報漏洩の分類

１章では企業のセキュリティに対する現状と問題点について見てきた。そこで２章において情報漏洩とは外部からのウイルスやハッキング等によって起きていると考えられがちだが、実際は社員が情報を持ち出していたり、社内におけるセキュリティの甘さから起きている内部犯行が７割とも言われている。このような現実における、実際内部からの情報漏洩と外部からの情報漏洩と言う二つの面から不正行為を考えたい。

１．内部のミスにおける情報漏洩

情報漏洩の可能性として、企業内部における操作、処理ミスがある。たとえば、メールの送付先を間違えてしまったり、添付ファイルを間違ってしまったり、さらには、オフィスに鍵をかけ忘れて侵入されてしまい、情報を盗まれたり、ＰＣの画面 を開きっぱなしで放置して情報を見られてしまうことも、書類を机の上に置いたままにして内容を見られてしまうことも、ファイルを誤って削除してしまったりすることもここに含まれます。それに、社内情報システムのメンテナンスを行っていると、ミスによってシステムを停止してしまい、復旧が必要になることもある。具体的な事例として以下の例が挙げられる。

・ **管理者による人為的ミスの事例**

会員制サイトやオンラインショッピングサイトでは、ユーザーが個人情報を送信して、サイト側がそれを管理することによって取引が成り立つ。厳重に管理されているはずの個人情報が人為的ミスにより流出してしまう事件がこれまでに何件か発生している。2000 年3 月には、大塚製薬の健康チェックのページに登録したユーザーの氏名、住所、年齢、電話番号などおよそ9000 人以上の個人情報が同社サイト上に約2ヶ月間放置され、検索エンジンなどを利用して簡単にアクセスできる状態になっていたことが発覚した。また同年同月、アメリカでは生命保険サイト「ＳｅｌｅｃｔＱｕｏｔｅ」で生命保険の試算表を得るために入力したユーザーの個人情報がソフトウェアの問題により、次に利用したユーザーの画面に氏名や住所、病歴などのデータが表示されるという事件も発生している。2000 年4 月に、ＮＴＴ－Ｘが運営する検索サイト「ｇｏｏ」のフリーメールサービスを利用するためのＩＤやパスワード435 人分が他の利用者に混入して送信されるという事件が発生したが、これはシステム更新作業中に起こった人為的ミスだった。このケースでは、流出したのはＩＤとパスワードだけで個人情報は漏れていないように思えるが、実はｇｏｏではこのＩＤとパスワードを使って、他の登録ユーザーの住所、氏名などの個人情報を閲覧することが可能となっていたのである。こうした人為的ミスによる個人情報流出は、それを閲覧する立場からすれば違法性がないので、拡散しやすい性質がある。特に電子データは複製を作りやすいので、ひとたび広がってしまったら対策をとるのは、特に個人では不可能である。

２．内部からの不正行為

情報漏洩事件の 7 割は内部犯行であるともいわれている。また過去に就業していた人物が嫌がらせ目的で外部から不正アクセスを行った、ウィルスメールを送ったりしていた、などという事例もある。これを防ぐためにユーザーに必要以上の権限を与えないことや、アクセスを制御することである程度の防衛策にはなるが、意図的な情報漏洩などは内部の人間には極めて簡単なことである。すでに退社した人間のアカウントやＩＤを消去することも必要である。

（1） 個人情報の漏洩

企業の人為的要因によって起こるデータの流出のことである。具体的なパターンとして以下の事例が挙げられる。

・ **データベース運営者側の内部犯行**

データベース運営者側からの内部犯行による情報の漏洩は、名簿屋と呼ばれる個人情報を売買する業者との取引を目的としたものがほとんどである。国内でもっとも大規模かつ網羅的な個人情報データベースを保有するのはＮＴＴであると思われるが、そのＮＴＴでは内部犯行による個人情報の漏洩が頻繁に起きている。1999 年5 月には姫路営業支店の社員が電話番号500 人分を売っていたことが発覚したことを契機に、内部調査をしたところ、同年9 月にはＮＴＴ西日本佐賀支店の若手社員が顧客10 人分の情報を現金5 万円で横流ししていたこと、10 月には東京支店の社員がダイヤルＱ２ の事業者に顧客の個人情報を流していたこと、ＮＴＴ　ドコモでは社員と派遣社員が顧客の個人情報を知人に流していたこと、同年11 月には、ＮＴＴドコモ社員とＮＴＴ東日本の社員が顧客データを過激派組織「革マル派」に流していたことが次々に発覚した。悪質なのは、姫路営業支店でのケースで、個人情報をインターネットのｗｅｂサイトでも売買していたことが分かった。この事件は個人情報のネットでの売買が摘発された初めてのケースとなった。

（2） Cookie によるプライバシーの侵害

多くの商業サイトではCookieという仕掛けを利用して個人のWeb利用動向を追跡調査している。そして商業サイトはこの Cookie を利用する事で、ユーザーの訪れたページやその回数、購入した商品など客の嗜好を調べる事が出来る。しかし意図せず個人情報が流出する場合がある。

・ **Cookie による情報利用の事例**

アマゾンドットコム社は、2000年8月から9月にかけて、2300万の顧客に自社のプライバシー政策の変更について電子メールで通告した。その内容は「我々は取引を推進するにあたり、店舗や資産を売買する場合があるかもしれない。そのような取引にあっては、一般的に顧客情報は継承商業資産である。また、そんなことは起こらないと思うが、アマゾンドットコム社や会社の実質的全資産が（他社に）取得される場合には顧客情報は継承資産の一部となる。」つまり、同社が収集した個人情報は同社の資産であるから、他の種類の資産や店舗などと同様、他社に販売するかもしれないのは同社の自由であり、また、買収などによって同社の資産が他の企業に移る場合には、当然個人情報もそれに伴って移転される、という内容のものであった。その結果、当然ながら電子プライバシー情報センター（ＥＰＩＣ）や顧客から強烈な反感を買うに至った。アマゾンドットコム社は、この

認証システムによって収集した個人情報を活用して種々なサービスを展開している。すなわち、容易な検索、書籍の内容紹介、顧客による書評、過去の購買履歴から読者の傾向を類推して自動的にいくつかの書籍を推薦する推薦システム（同じ分野または著者の本を3冊紹介）、注文後の読者への電子メールによる連絡（①注文確認メール②出荷通知メール＝同時に手配中のものの情報）をすべて自動的に行っている。このシステムに特許をとって競争相手をたたく手段としていることは批判を浴びているが、ターゲット･マーケティングをうまく活かしていることは注目に値する。　アマゾンドットコム社によるプライバシー・ポリシーの変更については、アマゾンドットコム社とＦＴＣ（Federal Trade Commission：米連邦取引委員会）が協議を重ねた結果にもとづき、2001年5月に、FTCは次の趣旨の書状を電子プライバシー情報センター（ＥＰＩＣ）と他一団体に対して送った。「たしかに変更後のポリシーの内容は曖昧なところはあるが、予め第三者への情報提供を一切認めない意向を登録していた消費者に関しては、個人情報を第三者に提供しないとの方針をアマゾンドットコム社は示した。そしてアマゾンドットコム社はＦＴＣに、過去において顧客の個人情報の販売、交換、貸与は一切行っていないと報告した。またアマゾンドットコム社は今後とも、顧客の事前の承諾なしにはこれを行わないといっているので、連邦政府が定めた取引方法に違反しなかったと考える」と述べた。

３．外部からの不正行為

近年、外部から攻撃される可能性は飛躍的に増えた。この背景には、なんと言ってもインターネットの普及が挙げられる。外部から送られてきたコンピュータウィルスはメールによってあっという間に広がるし、社内システムをインターネットにつないでいる限り､必然的に外部からの攻撃の可能性は増えることになりかねない。しかも、ハッカーによる侵入という行為そのものは考えているよりも簡単に可能である、というところが最大の問題なのである。これらを防ぐためにはこまめにシステムのチェックをし、セキュリティホールの修正を行うしかない。

また正規の手続きを踏まずに不正にコンピュータを操作することで、悪意のある者がいる限りデータが不正に持ち出されたり勝手に改ざんされたりといった可能性は排除できない。近年では多くのコンピュータがインターネットに接続されるようになったために、不正アクセスが深刻になっている。

具体的な不正アクセスの方法としてスキャニング、ＤＮＳゾーン攻撃、ＲＰＣへの攻撃、ＩＣＭＰ攻撃、ＤｏＳアタック、ＳＰＡＭメール、メール爆弾、バッファオーバーフロー、ウイルス、パスワードクラックなどが挙げられる。それぞれどのようなものかここで簡単に列挙しておく。

① スキャニング

攻撃対象のシステム／ネットワーク構成、導入ソフト、ＯＳなどの情報を探り攻撃の糸口を探る。

② ＤＮＳゾーン攻撃

スキャニング同様に、踏み台に利用できそうなサーバ情報を一括して探る。（ＤＮＳ：Domain Name Service）

③ ＲＰＣへの攻撃

外部から内部のシステムをコントロールできる機能（システムが正規に持っている機能）を不正に利用し、バックドアを作成したり、機密情報を抜き出していく攻撃である。

④ ＩＣＭＰ攻撃

攻撃対象のネットワークに、そのネットワーク上では扱えない基準のデータを強制的に送りつけてシステムを停止させる攻撃である。

⑤ ＤｏＳアタック

サイトの許容量を越えるデータやアクセスを送り込み、サイトの機能を低下／停止させサービスを妨害する攻撃である。

⑥ ＳＰＡＭメール

業務やサービスに全く関係のない、広告宣伝／勧誘のメールを送りつけ相手業務を混乱させる攻撃である。

⑦ メール爆弾

自動化ツールや踏み台を利用し、大量（数千～数万通）または大容量のメールを送信し、サーバの機能やメールアカウントを麻痺させる攻撃である。

⑧ バッファオーバーフロー

特に管理者権限で動作するプログラムのメモリ領域に侵入。故意に長いデータを送りつけメモリにオーバーフローさせプログラムを誤動作させる攻撃である。

⑨ ウイルス

プログラムやファイルに埋め込まれた悪意のあるプログラム、多くの種類が出回っており、メールやデータ転送などにより感染する。

⑩ パスワードクラック

パスワードとして使用されがちな単語や文字の辞書を用意し、ツールにて総当りを行い、パスワード解読を行う。

現在インターネットを介してのビジネスが広がる中で、内部のセキュリティに対する意識や不正行為の危険性が内在している点にも注意する必要がある。

第３章 企業における情報漏洩の対策

３章では、まず２章で述べてきた不正アクセス行為に対して実質的に対抗するためのセキュリティ技術についてふれ、次に情報セキュリティポリシーの策定や企業におけるセキュリティ教育について考えていきたい。

１．セキュリティ技術

２章でも述べた不正アクセスに対応するための技術的なことに関する現在ある技術についてまず考えたい。

① ワンタイム・パスワード

不正ログインに対抗する技術として挙げられる。システムにログインする際には使い捨てパスワードを使用し、そのパスワードはワンタイム・パスワード生成器などを用いて生成する。使い捨てパスワードなので、しらみつぶし的手法での攻撃は無効であり、また専用のアルゴリズムにより生成されるパスワードなので、使用するユーザーに左右されないため、パスワードの推測は、ほぼ不可能である。

② ファイアウォール

これは外のネットワークに対して中のネットワークの周りに防護壁を築くものであり、アクセスに際しては本人確認を必要とし、更に外からのアクセスに対しては可能な行動を限定するものである。ソフトウェア的な対応、物理的な対応など、場合に応じて様々な構築方法がある。しかし一般に防護壁を高くすると利便性が低くなるため、バランスをどうするかが問題である。

③ 暗号化

インターネットはその構造上、電子メールなどのデータの中身を"盗み読み"されてしまう可能性がある。これを防止するには、メールをやり取りする者同士で暗号技術を用いた「暗号メール」を用いることが有効である。暗号メールとしてはＰＧＰ、Ｓ／ＭＩＭＥなどが広く知られている。ウェブを利用した電子商取引においてはクレジット番号など第三者に悪用される危険性をもつ情報が、ネットワーク盗聴などにより詐取されるようなケースが考えられる。この問題は、ネットスケープ・コミュニケーションズ社が提唱している「ＳＳＬ（Secure Sockets Layer Protocol）」などを用いることによって、リスクを回避できる。ＳＳＬは、サーバとブラウザ間の通信を暗号化し保護する。暗号化された通信内容を攻撃者

が解読することは現実的なレベルにおいて不可能である。このように取引サイトに対しクレジット番号等の情報は暗号化されて送信されるため、経由するネットワーク上からの情報漏洩のリスクが激減する。

④ 侵入検知システム（ＩＤＳ）

ＩＤＳ（Intrusion Detection System）インターネットからの不正アクセスなどを検知し管理者に警告を出したり、トラフィックを遮断する機能や機器である。主に侵入パターンとネットワークやマシンの利用状況から不正アクセスを検出する。侵入パターンとは、一般的に行なわれている不正アクセス特有のトラフィックを現わしており、シグネチャ（Signature）とも呼ばれる。

たとえば同時期にＴＣＰポートの接続失敗が多数発見された場合は、ポートスキャンを行なっていると判断する。一方、ネットワークやマシンの利用状況による検出は、たとえばＣＰＵの利用率が１００％に達して長時間下がらないとか、ユーザーのログインの失敗が短期間に複数発生しているといった事象から、不正アクセスを見いだす方法である。いずれの方法にしても、不正アクセスのトラフィックを確実に検出できるというわけではない。

しかしＣＰＵやメモリなどのリソースを消費させることでサービスを停止に追い込むＤｏＳ攻撃やＯＳやプロトコルの不具合を狙った古典的な不正アクセスにはかなり有効である。ハードウェア、ソフトウェアなど製品はさまざまだが、ファイアウォールとルーターの間に設置されるゲートウェイとして機能するものが多い。

また、リアルタイムに侵入検知を行なうものと、ログを精査することで不正侵入を発見するものの２種類がある。

２．情報セキュリティポリシーの策定

セキュリティ技術にて外部内部問わないセキュリティ技術について取り上げてきた。そして情報セキュリティポリシーの策定では、会社内部からの情報漏洩をなくすための方法として会社が全社的に取り組むべきセキュリティポリシーの策定について考えたい。

情報セキュリティポリシーとは組織の情報セキュリティに対する考え方や取り組みにおける原則、基本方針などが盛り込まれたものという意味で使うこととする。

ネットワークセキュリティにおいて企業が守るべきものは何かと考えてみると、顧客の情報、社員の住所録などの個人情報、重役会議の資料、新製品の企画書な

ど、例を挙げるときりがないが、これらすべてに共通することは、企業の「情報」である。「情報」は企業にとって重要な「資産」であるのだが、この「情報資産」という考えが根付いていないため、守るべきものが何であるのかを見誤ってしまうことが多々ある。しかし、例えば、物理的に誰かが会社に侵入しコンピュータが盗まれたとして、その損害を考えたときに、本当に損害が大きいのはコンピュータ自体よりもむしろコンピュータの中に入っている「情報資産」を盗まれたことであるはずである。つまり、本当に守るべきものは企業の「情報資産」なのである。また、セキュリティというと、一般的にはコンピュータのネットワーク上にある情報漏洩の危険性などが示唆されるが、企業が守るべき「情報資産」は必ずしも電子的なものではなく、情報を印刷した紙、ひいては人間が話す話の内容などさまざまな形態で存在する。

そして一昔前のように企業のネットワーク管理者のみがセキュリティ対策を行えばよいという時代ではなく、ユーザー1 人 1 人がセキュリティ意識を持ち、全社的なセキュリティ対策を実施していく必要性が増してきている。また企業の情報資産は、ユーザーの認識不足や外部からの不正アクセスなどによるものだけでなく、内部犯行という大きな脅威にもさらされている。それは不正に内部の人間と同じ資格を得た人間もさることながら、正社員、契約社員、派遣社員、アルバイト、パートタイマーなどによる情報資産の漏洩は回避することが非常に難しい。未だ内部犯行に関して意識が低く、まさか内部の人間がそのようなことをするはずがないなどと思っている。それが実際社会的に問題となった情報漏洩事件が内部犯行である場合も少なくない。

そこで情報セキュリティポリシーを整備し、物理的な入退室管理や、適切なアクセス制御を実施し、またユーザーのセキュリティ意識レベルを上げることで、内部犯行を未然に防げる可能性は飛躍的に高くなる。

3．セキュリティ意識を向上させるための教育

例え情報セキュリティポリシーを策定したとしても実際に運用を実践するのは人間なので、運用を成功させるためにも教育の必要性が問われてくる。そこで情報セキュリティを教育する上で「何をなぜ守るか」と「どうやって守るか」といった 二つの切り口から教育を考えたい。

（1） 何をなぜ守るか

この教育は情報を扱う人間に一様に実施する必要がある。ここでの重要な点は事業において情報がいかに大切であるかを認識することが一番重要なことである。

それは「情報が第四の経営資源である」と言われるようになって久しいですが、未だ感覚的に情報の価値に対する認識が薄いと言って過言ではない。そこで事業における情報の価値を理解させる意味で必要なのである。

（2） どうやって守るのか

この教育は必ずしも情報を扱うすべての人間に実施する必要はない。それは各自の業務の内容によって変わる可能性が高い。ではこの教育を行うのかと言うと、日常の業務の中で情報セキュリティを守るようにする下地を作る意味で必要なのである。

このように情報セキュリティに対する意識を高めて運用を円滑化していくために前述のこと以外に、トップダウンで情報セキュリティの重要性を訴え続けることが挙げられる。そうすることで情報を保護するという意識が高まるのである。

第４章 現状で企業が出来る情報漏洩に対する対応策

３章で現在の技術的なことと情報セキュリティポリシーに対する企業の取り組み方や全社的に社員にどのような対策をとるべきか述べてきた。そして４章で最新の技術や通信業界における現在対企業用に販売している商品を通して、現在の企業は情報漏洩に対してどのような対策をとっているのか考えたい。

１．最新の技術

不正侵入防御システム（ＩＰＳ）

不正アクセスの検知と防御を 1 台の装置で自動的に行えるのが特徴だ。ファイアウォールのように特定のプロトコルを通さないように設定したり、通信を許可したプロトコルであっても不正侵入検知システム（以下ＩＤＳ）のようにトラフィックの中身を分析して不正と判断した場合にはポートを閉じるなどして遮断する。こうした課題に対応し、ファイアウォールと IDS の機能を言わば一体で提供するのが不正侵入防御システム（Intrusion Prevention System）である。

２．現在の対企業向けセキュリティ商品

４章の冒頭でも述べたとおりここでは通信業界におけるセキュリティ商品を見ることを通して現在のセキュリティのあり方を考えたい。

（1）NTTコミュニケーションズのGuardITの場合

情報資産を不正アクセス、情報漏洩などさまざまな脅威から守るためにセキュリティポリシー策定を含むコンサルティングからセキュリティシステムの設計、構築、そして日々の運用管理まで全てを一元的に提供している。

具体的には、ファイアウォールの管理、不正アクセス監視、セキュリティホール調査、ウイルス対策、内部情報漏洩対策などのシステムの部分だけを行うのではなく、セキュリティポリシーやBS7799やISMS認証取得に関する支援なども行っている。

（2）KDDIの場合

ウイルス対策、セキュリティ監視、ファイアウォール運用管理、電子認証局構築、セキュリティポリシー構築支援等のサービスを行っている。

このように現在通信業界においてただセキュリティ技術の向上を計るだけではなく、情報セキュリティをトータルで考えるようになってきた。そして企業も情報資産を一括管理することでセキュリティ対策をとっているのが分かる。

第５章　今後考えられる情報漏洩の危険性とその対策

１章で情報漏洩の現状について、２章でネットワーク全体を介した情報漏洩の実態、３章で企業の対策の現状、４章では最新のセキュリティ技術や対企業で現在どのような商品があるのかを挙げてきた。そして５章では、今後より発達するインターネットにおける技術と新たな情報漏洩の危険性を示す一例としての無線LANについて取り上げる。そしてその危険性はどのようにしたら回避できるかを現在ある技術から対応策を考えていきたい。

１．インターネットの新たな技術における情報漏洩の危険性

近年、無線LAN機器の低価格化、オペレーティングシステムが無線LANを標準サポートした事による設定の容易化などで、無線LANが企業・家庭に急速に普及してきている。無線LANは有線LANに比べてどこでも作業でき、配線費用の削減、ケーブリングトラブルの軽減、迅速なLAN構築が可能等のメリットがあるため今後ますます普及していく事が期待される。

（1）無線ＬＡＮ

有線ＬＡＮ接続では、ユーザーは直接ＬＡＮケーブルにＬＡＮアダプターを介して接続しなければならない。しかし無線ＬＡＮでは、無線電波の届く範囲であればオフィスや家庭内でなくても、ＰＣに接続された無線ＬＡＮカードで無線電波を受信し、ＬＡＮ接続をおこなうことができる。電波の届く範囲であれば自由にＬＡＮ接続が可能であることは無線ＬＡＮの利点だが、だからこそ情報漏洩の危険性も高いといえる。

（2）無線ＬＡＮの問題点

無線ＬＡＮは配線の手間なしに簡単にＬＡＮ環境を構築できるように、無線ＬＡＮを搭載したパソコン、無線アクセスポイントは特別な設定なしに全ての装置が相互に通信ができるように設計されている。しかし電波はある範囲内であれば障害物を越えてすべての場所に届く。そのためセキュリティに関する設定を行っていない場合、通信内容を盗み見られたり第三者が無断で個人や会社内のネットワークへアクセスして、個人情報や機密情報を取り出す情報漏洩が起きる。また特定の人物になりすまして通信し、不正な情報を流したり、傍受した通信内容を書き換えて発信したり、コンピュータウィルスなどを流しデータやシステムを破壊するなどの行為が行われる可能性がある。そこで無線ＬＡＮには有線のＬＡＮ以上にセキュリティ対策が必要と考えるべきである。

２．今後企業における情報漏洩を防ぐためにどうすればいいのか

近年情報技術の向上によってビジネスのスピードが急速化や、個々の情報への的確な対応が必要になってきた。また企業はビジネスを円滑、効率的に運営する上で、ネットワーク技術の重要性は高まるばかりである。ただそのような利便性が唱えられる半面、企業の情報システムに対する不正アクセスの件数も急激な勢いで増加している。このような被害にあうことで企業自体の社会的信用を失ってしまう状況に陥ることがある。このように情報セキュリティに関する損失から企業を守るためには、技術的な対策だけでなく全社的にセキュリティ教育を行うべきである。

また今後より利便性を求めてインターネット技術は進歩していく。その過程

である無線ＬＡＮだが、セキュリティ機能の設定を全く行わないまま無線ＬＡＮを使ったために、通信の内容を盗み見られたり、自分のパソコンに他人が侵入したといった情報漏洩に関する事件が最近おきている。無線ＬＡＮのセキュリティ保護は非常に重要な問題であり、これを技術的な分野だけでなく、企業的にはセキュリティに対する教育を取り組むことが必要である。

　このように今後技術が発展していく中で、より情報漏洩の可能性は広がっていく。そこで企業は現在環境保全に対して取り組むのと同様、今後情報教育の拡充を行う必要性が問われてくるはずである。

【参考文献】

著：監査法人トーマツ
『セキュリティ・マネジメント戦略』ISMS によるリスク管理　　／日本経済新聞社

著：小泉修
『インターネットのすべて』／日本実業出版社

監修：赤堀侃司
『標準パソコン用語辞典』　／秀和システム出版編集部

【参考ＵＲＬ】

無線ＬＡＮのセキュリティに関するガイドライン
ＵＲＬ：http://it.jeita.or.jp/perinfo/committee/pc/wirelessLAN/index.html

ＩＴＰｒｏ
ＵＲＬ：http://itpro.nikkeibp.co.jp/

月間情報セキュリティ
ＵＲＬ：http://www.monthlysec.net/

ＮＴＴコミュニケーションズ
ＵＲＬ：http://www.ntt.com/index.html

ＫＤＤＩ株式会社
ＵＲＬ：http://www.kddi.com/index_h.html

情報セキュリティ入門
ＵＲＬ：http://www.atmarkit.co.jp/fsecurity/rensai/policy11/policy01.html

経済産業省　商務情報政策局　情報セキュリティ政策室
ＵＲＬ：http://www.meti.go.jp/policy/netsecurity/index.html

独立行政法人 情報処理推進機構
ＵＲＬ：http://www.ipa.go.jp/index.html