ラウンドテーブル

インターネット時代の情報リスクの実態と通信事業者の課題

イーフラッグコンサルティング 代表
(㈱インターリスク総研 コーディネーター)

田中（たなか）　克政（かつまさ）

tanaka@eflag.co.jp

本日は、このような席にお呼びいただきましてありがとうございます。短い時間でございますけれども、情報セキュリティに関してお話をさせていただきます。

情報セキュリティというお話をしますと、難しい話だとか、技術的な話が、どうしても中心になる傾向があるのですが、本日は、どちらかというとマネジメントというか、経営の観点から、特に情報のリスクに関して、みなさまのヒントになるようなお話ができれば幸いと思っております。最近、特にいろいろな事件が起きておりますが、そういう話ですとか、実際に企業から相談を受けた内容を中心に、具体的な事例をお話ししていこうと思います。

昨日も名古屋で講演がありまして、大手企業を中心に、経営者の方に対してお話をさせていただいたのですが、そこでも話が出たのですけれど、みなさん、よく、失われた10年と言われます。その失われた10年間をよく見てみますと、携帯電話のようなものは、私の記憶ですと、1953年の船舶電話からスタートして、もう50年以上の歴史があり、この10年の間に5,000万台という数字まで普及してきています。NTTドコモの話ですと、あと10年の間に8,000万台、人口で言いますと60～70%以上の普及を目指しているということです。

その情報通信、俗に言う「IT革命」は、アメリカの影響で終わったのではないかという話が昨日もあったのですが、実は、まだ日本ではIT革命は来ておりません。どうしてそういうことが言えるのかというと、企業自体の競争が、インターネットなど情報通信を中心にした競争にまだ移っていないからです。

具体的に申し上げますと、企業自体の競争というのは、国際的な競争、例えば同じ商品であれば、アメリカのほうが高いとか、安いといったこと。それから企業間の競争、ユニクロと一般の洋品メーカーであれば、ユニクロのほうが安く作れるので強いといったこと。もう一つは社内での競争。この三つがあるのですが、この競争のポイントは、情報化のスピードであり、情報化に対応できた企業なり人間が勝つ、つまり情報が中心になってきているのです。

リスクに関してのお話をする前に、リスクというのは具体的にどういうことかと申しますと、今の企業の競争という話の中で、リスクを取っていく者が勝った場合に、「リスク競争に勝った」という言い方をします。

具体的な話をしますと、今度、11月にコムデックスというアメリカのイベントに行くのですが、コムデックスはラスベガスのホテルでやるわけです。そのショウのチケットを取るのが非常に大変で、2～3年前からやっとインターネットで予約できるようになり、日本から予約をするのですが、そのときクレジットカードの番号を送らないといけないのです。危険だと思いながらもクレジットカードの番号を送るわけで、そうやってチケットを買えた人間が、そのショウを見ることができるのです。ショウを開催するラスベガスのホテルの力が強いので、リスクをユーザーが取らなくてはいけないわけです。

先ほどの話に戻りますと、今後、リスクをどちらが取るのだということになった場合、情報の分野においても、力の弱いほうがリスクを取らざるを得ないという世の中に変わっていきます。それがユーザー対企業なのか、企業対企業なのかは別として、そういう傾向があります。

インターネットのリスクの中で、今、問題になっている点をいくつか挙げて説明していきますが、情報通信の分野で言いますと、地方へ講演に行ったときに問題として出てきたのは、地方のプロバイダーが競争に直面して、つぶれるか、つぶれないかという状況になったとき、セキュリティ対策を削って、サービス料を下げるしか選択肢がないのではないか、という相談を受けました。

私がこのビジネスを始めた4年前、福岡のハッカーのところ

に行ったことがあります。今は不正アクセス禁止法という法律ができておりますけれど、NHKの『クローズアップ現代』という番組の記者も一緒に行き、そのハッカーと半日ぐらい一緒に過ごして、実際に不正アクセスの現場を見たわけですが、当時、プロバイダーの8割に侵入することができました。ハードディスクの中に、プロバイダーごとのIDファイルが入っていて、「では、これから不正アクセスをします」と言うと、そのハッカーは適当にIDとパスワードを選んでプロバイダーに侵入していくわけです。

「今度は会社から入ってみましょう」と言って、モデムから電話をかけて、その企業に侵入していくのです。

その企業に侵入するのが目的ではなくて、その企業を経由して、別の会社の情報を取るためにやるということで、当時、ハッカーは何の目的でそれをやっていたかというと、自分の接続環境を無料にするためというのが第一義的にあるのですが、技術的な競争、自分の興味本位でやっていたという傾向がありました。

実際、海外でも同様な状況がありまして、米国の場合ですと、ハッカーが集まるイベントがあり、昨年は約4,000人のハッカーが集まり、ハッカーコンテストをやったり、ハッカーのツール、CD-ROMを売っていたりするわけです。アメリカだけでその調子ですから、今後、東南アジアや中国の人たちがITに強くなってくれば、世界中で常時、約2万～3万人のハッカーが、何らかの攻撃を弱い企業、弱い国に仕掛けてくる可能性があります。

そういうことで、アメリカでは3,000億円からの予算で防御体制をとろうとしていますが、日本の場合、せいぜい100億円か200億円の範囲で一生懸命やっているにすぎません。

私が、ある官庁向けの教育に携わったときの話ですが、そこの上司の心配事は、教育が終わった後、大手のIT企業に転職してしまうのではないかと気にしていました。

別の官庁に行ったときも、まったく同じことを言われて、IT業務にかかわる人材の中途採用募集をかけると、人は集まってくるのだけれども、優秀になった後、その人間が他に逃げる可能性が極めて高い。それを抑える方法はないかという相談を受けて、契約書で縛ってもなかなかそれは難しいので、不可能ではないかという話をさせていただいたのですが、官庁側にも、そういう問題点が出てきております。

FBIの調査の資料等を見てみますと、セキュリティに関する問題点は、方向性がだいぶ変わってきています。最近でも、ウイルスだとか、不正アクセスでホームページが書き換えられたという話をお聞きになったことがあると思うのですが、具体的な数字でいきますと、日本の企業のホームページが、1日で5～10件ぐらい書き換えられております。

実際に、そういうホームページが公開されて、ここが書き換えられたという情報が見られますし、その企業の名前も出るのですが、ほとんどが地方を中心とした中小企業、それと社団法人とか財団法人のような、いわゆる政府の管理の下で運営されている活動団体のホームページが書き換えられています。

原因は何かというと、先ほどの地方の話にもありましたけれど、いわゆる予算がないということです。システムの構築で予算を使い切って、保守とかメンテナンス、セキュリティ対策ができないというところが原因になっています。

そういう不正アクセスに関するリスク、特にお金を失うという意味で言いますと、情報が漏れることで訴訟や損害賠償請求を受けたり、信用を失ったりするリスクに対応した保険が出てきておりますが、逆にいうと、保険が出てくるほど一般化してくるという傾向がありまして、特に問題になっておりますのは、先ほどFBIの話をしましたが、セキュリティ犯罪の55％以上が内部犯によるもので、アメリカのセキュリティ会社の調査によると80～90％が内部犯という調査結果もあります。

非常に大きな事業者からセキュリティに関する相談を受けたときに、こういう話がありました。「社員が2,000人いると、1人や2人、悪いのが必ずいる。それをどうやって見つけたらいいですか？　システムで見つけますか。人事の仕組みで見つけますか?」という相談を受けまして、非公式に伝えたのは「社内でお金に困っている人がいたら、その人には○印を付けておいてください」と、まじめに話をさせていただきました。

というのは、そうした不正犯罪の中で、特に内部犯が情報を漏らしたうちのほとんどが情報を売ってサラ金にお金を返すとか、そういうものがほとんどなのです。50万円とか100万円で名簿を売ったりして、直近の借金を返すことに使っているのです。

アメリカでは50％が内部犯という話で、日本ではまだ1～2割と少ないですが、今後、非常に増えてくる可能性があります。特に中小企業など、情報に関してあまり対策がとれないような企業を中心に、こういう部分が広がってくると思います。

情報リスクに関する具体的な数字であるとか、状況であるとかは、日々刻々、変化しており、特に今年に入りましてウイルスだとか、不正アクセスが非常に増えていることは実感されていると思いますが、小さな企業を中心に大きな被害が今後、出てきそうです。不正アクセスの被害はまだ受けていないとか、うちは関係ないと言っている会社であっても、会社が伸び、調子が良ければ良いほど、ますますその脅威は大きくなってきます。

ここにお集まりのみなさまは、情報通信関連やシステムベンダーのプロの方が中心だと思いますが、みなさま方に、ぜひお願いしたいのは、みなさまが、いろいろな企業の方にお会いになられる中で、その部分について相談をお受けいただい

て、「不正アクセスは怖いですよ」ということを、ぜひ強くお伝えいただきたいのです。

それと同時に、もし覚えておいていただければ、保険であるとか、私どもコンサルタントのようなプロの集団も出てきておりますので、私どもに相談いただいたり、保険の手当て等もお考えいただければと思います。

最後に、お集まりの通信事業者のみなさまにとって、これから先最大の脅威は何かをお話しして終わりにしたいと思います。

詳しい人もおられると思いますが、最近、“コードレッド”というウイルスが流行しました。これはどういうウイルスかと言いますと、マイクロソフトのサーバーを発信源として、インターネット通信上に大量に情報を投げる形のウイルスです。

このウイルスに感染しますと、通信線上に関係のない情報が大量に流れます。私のよく知っているプロバイダーもだいぶ被害を受けましたが、どういう被害かと言いますと、ウイルスに侵されるのではなくて、通信線自体がコードレッドの情報で埋まってしまうのです。これは新しいタイプの攻撃というか、脅威でございまして、例えて言いますと、せっかく作った道路の上を暴走族がガンガン走り、一般の通行者が通れなくなってしまう状態です。そして、その暴走族を抑える方法、摘発する方法が、なかなかありません。理由は、一般の情報とウイルスによる情報の区別がインターネットでは、つきにくいためです。

今、通信のブロードバンド化が進もうとしていますが、ウイルスにより妨害通信のような、そういうゴミと業務上の有益な情報が、インターネットで区別できないために、通信設備に過剰な投資が必要になっている場合があります。例えば、個人のインターネット利用のうち、日本ではかなりの部分がポルノ情報の閲覧であるという説もあり、そういうものも含めて減らすことができれば、通信設備費のかなりの無駄が省けるかもしれません。通信線を占領する不正なアクセスへの対策なしに、今後のブロードバンドの発展は難しいことと思います。ですから、通信事業者でお働きになっている方にお願いしたいのは、ブロードバンド化と併せて、通信データのセグメント化による良質な情報の分離や、セキュリティの強化を、今後いっそう研究していただきたいと思います。

ご清聴ありがとうございました。

（305回ITUクラブ例会より）