情報セキュリティを確保するための意識改革について

研究員　小島　和浩

1　はじめに

オレオレ詐欺が世間一般に認識されてからもう何年にもなりますが、各種対策が取られているにもかかわらず一向に被害が減る傾向にはなく、むしろ増え続けています。毎日のように新聞のどこかに報道があり、調べてみると平成２６年７月中だけで、被害総額が１７億円を超えているとのことでした。

オレオレ詐欺といえば、振り込め詐欺だと思う方が大半だと思いますが、実際に起こった平成２６年度上半期の被害状況をみてみると、いわゆる振込型が約１割、現金等を直接受け取る現金受取型が約８割となっていました。今では、「『振り込ませない』振り込め詐欺」が手口の大半を占めているということを、皆さん知っていましたか。

もし、皆さんが本気で振り込め詐欺の被害をなくそうと思うなら、犯行の手口が年々進化（発展を意味する言葉は使いたくありませんが、適当な言葉が見つからないので・・・）しているということを知ることが大切です。自分勝手にオレオレ詐欺はこんな手口だと思うのではなく、振り込め詐欺に対する見方を改め、きっちりと実態を把握した上で、詐欺に対応するという意識改革が必要です。

情報セキュリティの分野でも同じようなことが言えます。情報漏えい等の事案が時々ニュース等で報道されますが、その犯行の手口は外からの攻撃によるものであったり、内部犯の仕業であったりと様々です。でも、最近の攻撃の傾向や新たな手口の実態を知り、しっかりと対策を取っていれば、防ぐことが出来たケースが大半のように思われます。セキュリティ対策の必要性は、担当者たちには十分理解されているはずなのですが、適切な対応が取られていないのは、周りの人たちの理解が低く危機意識が薄いからではないでしょうか。

この問題を解決するために、関係するすべての人たちを巻き込み、組織全体でセキュリティ対策が取れるように、現在発生している深刻な被害の状況とこれまで起こってきた攻撃の変遷を紹介し、現状の理解と危機意識を高め、その中で一人一人がそれぞれの立場で情報セキュリティを確保するために行うべき意識改革の方法について述べたいと思います

2　深刻な被害状態

最初にオレオレ詐欺の被害状況を紹介しましたが、情報セキュリティの分野でも、今不正送金被害が深刻な問題となっています。警察庁のレポートによると、平成２３年の被害総額が約３億８千万円だったものが、２４年に約４千８百万円に減少しましたが、２５年には１４億６百万円になり過去最多額を記録しました。更に、今年に至っては、５月９日の時点で１４億７千万円と４か月程で昨年

の被害総額を上回っているとのことです。

当然、銀行サイドは、ネットバンキングシステムのセキュリティ対策を実施しています。ユーザーのオンラインバンキングＩＤとパスワードがなければ、サイトにアクセスすることが出来ませんし、最近ではワンタイムパスワードの使用も既定化しておりセキュリティが強化されています。それでも、被害総額は昨年を上回るペースで拡大し続けています。

金融の被害は、届出等があり具体的にどれだけのお金が不正に窃取されたか分かりますが、企業の持つ情報資産についてはどれくらいの被害が発生しているのでしょうか。今年 7 月に発覚した教育事業会社における個人情報の漏えい事件のように、具体的にわかったものもありますが、表に出ないものの方が多いと推測されます。しかし、攻撃者が狙うものは、主にお金と情報なので、金融の世界でこれだけの被害が出ているということは、情報の分野でもかなりの攻撃が起こっていると考えられます。そして、一旦被害が公に出るような事態になると、単に被った被害だけにとどまらず会社の信用問題にまで発展し、その収束に多大な労力を払うことになります。シマンテック社のレポートによると、平成２５年は２４年に比べ、特定の組織や企業を狙う標的型攻撃が９２％増加しているとのことですし、まだ公表されていない未知の脆弱性をついたゼロデイ攻撃も１４件から２３件と倍増しています。

３　攻撃の変遷

この様なご時世ですので、ウイルス対策ソフトやファイヤーウォールの導入をしておけば、セキュリティ対策は大丈夫だと思っている方はいないと思いますが、それでも私たちが思っているより速い速度で攻撃の手口は進化していますので、常に新しい防御策を取り入れる必要があります。そのためにも、攻撃の手口がどんどん高度化･巧妙化していることに対する危機意識を常に持っておかなければなりません。

（１）金融機関への攻撃

金融機関を狙った犯行の手口を振り返ってみると、平成１６年ごろからサイト上で個人情報やＩＤ／パスワードを狙うフィッシング詐欺というものが日本国内で確認されました。１７年になると、コンピュータの入力情報を監視してＩＤ・パスワードといった認証情報を盗むキーロガーが出現しました。平成２１年には高度な認証情報(二要素認証)を盗む攻撃も現れました。２２年になると銀行の正規サイトが攻撃され、利用者がサイトにアクセスすると不正プログラムが正規サイト上で偽りの画面を表示する手法も確認されました。最近では、ワンタイムパスワードを突破する詐欺ツールも確認されており、ワンタイムパスワードを使っているから安心という状況ではなくなってきました。

（２）サイバー攻撃の変遷

情報セキュリティの分野においては、平成１３年から１５年ごろはネットワ

ークウイルスの全盛期の時代で、いたずらを目的とした攻撃が盛んに行われていました。マルウェアの一種であるワームという言葉も、広く一般の人たちにも知られるようになりました。１６年ごろからは、金融機関を狙った犯行で紹介したように金銭取得を目的とした攻撃が出現てきました。また、不正アクセスによる情報流出やスパイソフトウェアによる不正送金事案の発生が顕著化したり、個人情報保護法が全面施行されたのもこの時期です。平成２１年ごろからは、外部からの攻撃というものが注目され「サイバー攻撃」という言葉が一般化し、踏み台と呼ばれる多数のコンピュータを使ったＤＤｏＳ（Distributed Denial of Service attack）攻撃のような大規模な攻撃が行われるようになりました。平成２３年には、大手防衛産業へのサイバー攻撃事案も発生し、特定の組織や企業を狙うサイバー攻撃の一種である「標的型攻撃」が注目を集め始め、政府機関や企業から情報を窃取する事案が表面化してきました。標的型攻撃は、人が介在し遠隔操作により欲しい情報を窃取するものですが、ウイルスが主要な役割を果たすため、攻撃の第一段階として様々なテクニックを使いながら、標的とした相手方のパソコンにウイルスを送り込み感染させる手口が使われています。

ア　なりすましメール攻撃

ウイルスに感染させるために最も多く使われている手段は、なりすましメールによりウイルス付添付ファイルを送りつけてくる方法です。その添付ファイルを開かせウイルスを起動させるために、アイコンやファイル名の偽装という手段が取られ、さらにメール自身も送信者が実在する人物に詐称されており、政府の機関、取引先の関係者、友人知人を装ったメールを送りつけてくる事例が多く確認されています。一方で昨年からは、なりすましメールを警戒するシステム利用者が多くなったため、数回普通のメールをやり取りし、相手が安心したところでウイルス付メールを送る「やり取り型メール攻撃」も出現してきました。

イ　水飲み場型攻撃

最近では、標的とした相手方が良く使うウェブサイトを調べ、そのサイトに脆弱性があるとそこに攻撃を仕掛けて不正なプログラムに感染させ、標的となった者がそのサイトにアクセスしてきたときだけに別のサイトに誘導してウイルスを送り込む「水飲み場型攻撃」といわれる手口も出てきました。サイトの利用者は、正規サイトへのアクセスであり手続きが適正に行われたと思い込んでいますし、特定の人がアクセスしたときにしか不正プログラムが作動しないようにしているため発見が遅れるケースが多いようです。

ウ　パスワードに対する攻撃

また、パスワード、ＩＤを使って不正に侵入する手口も高度化しており、当初はパスワードとＩＤを適当に組み合わせた総当たり攻撃と呼ばれるものだったものが、ある程度考えられる組み合わせを使った辞書攻撃に進化し、

平成２５年にはより侵入確率の高いパスワードリスト攻撃が出現し注目が集まりました。この手口は、攻撃者がウェブサイト等から不正に取得したＩＤ／パスワードのリストを使い、複数のサイトで同一のＩＤ／パスワードを使っている利用者に対して不正アクセスを仕掛けるものです。今では、多くのサイトがログインするためにはＩＤ／パスワードを入力しなければならない設定になっていますが、利用者にとっては複数のパスワードを管理することが負担になるため、つい同じものを使いまわす人が多いようです。実際、ＩＤ／パスワードの組み合わせが３種類以下の利用者が７０％をこえるというアンケートの調査結果があります。

４　それぞれの立場でとるセキュリティ対策

実際に金融被害等が拡大していること、攻撃の手口が年々進化してきていること等が理解していただけたと思いますが、それでもまだ今は被害にあっていないからと他人事と思っていませんか。今後さらに攻撃の対象が広まっていくこと、もし情報漏えい等が起こった場合には社会的に大きく企業の信用を落とすこと等を考えると、組織を挙げて情報セキュリティ対策を講じることは必須の事項と言えますので、直ちに以下の改革に取り組む必要があります。

（１）公開宣言による関係者に対する強制的意識改革

一番重要なことは、関係者一人一人のセキュリティ意識の改革を図ることだと思います。具体的な活動はしていないけれど「セキュリティ対策は必要で、大切な情報を守らなければならない。」という認識を持っている方は多いと思いますので、それらの人達を行動に移させるような意識改革を図ることが必要です。そのためには、「内言語法」という自己暗示をかける手段を使います。意志は、「口に出して伝えて初めて意味を持つ」と言われますが、自分のやりたいこと、やらねばならないことを宣言させます。言葉として出した以上は、それを行うことについて責任が出来てきます。また、周囲の人たちもそのような目で見てくれるので、言ったことに対して活動を行うことについても理解が得られます。ほとんどの人が情報システムに詳しいわけではありませんし、どのような対策を取ればいいか分かっているわけではありません。しかも攻撃の手口はどんどん巧妙化しており、これらに技術的に対応するのは並大抵のことでできるものではありません。だからこそ、経営者、システム管理者、現場の取扱者それぞれが、単に「わが社の情報資産を守る」という意識を持つだけではなく、それを公言するという手段をとり、まずは行動を起こすことが必要です。いろいろと難しい状況であったとしても、動くことによって必ず解決の手段が見つけられます。ですから、決めたことややらなければならないことを心の中に止めておくのではなく、はっきりと宣言して周囲の人たちの理解と協力を得ながら解決をしていくことが大切です。

（２）役割別意識改革

ア　経営者等は先頭に立つ気概を持つ

情報セキュリティ分野における経営者等の果たすべき役割はかなり重要です。現在おかれている厳しいセキュリティ環境では、経営者等が良くわからないからと言って手をこまねいていることを許してくれるような状況ではありません。経営者等は、率先して前項で述べた「宣言」を行い、まずは核となる会社の情報セキュリティ方針又は改善策を打ち出し、それを必ず実行するという強い意志を示し、具体的な行動を起こさなければなりません。経営者等の年齢的なことを考えると、ＩＴ等に精通している方は少ないのではないかと思いますが、それでも今まで培ってきた経験や人脈を駆使して積極的に対策を打ち出し、セキュリティ確保に取り組む強い姿勢を示すことが必要です。経営者等のやる気や真剣さを感じると部下や組織は動きます。

イ　システム管理者の勇気

システム管理者のセキュリティに取り組む姿勢を改革できれば、積極的な提案が行われ強固なシステムを作ることが出来ます。情報システムは維持するだけでも経費が掛かるのに、さらにセキュリティを向上させるとなれば益々の負担増になります。ですから、具体的な生産活動の向上につながらないシステムの改善提案を行うことは厳しいものがあります。でも、そこであえてシステム管理の責任者である管理者が改革に取り組むという宣言を行い、システムの改善を行わなければなりません。一番現状や問題点を理解したシステム管理者が、本気でシステムの見直しを行えば、最新の技術を取り入れたセキュリティに強いシステムが構築できます。

ウ　取扱者の士気の保持

現場の取扱者がセキュリティ意識を強く持てば、規則等が確実に守られ正しい手順に基づいた業務が実施されます。人は慣れてくるとついつい手を抜きたくなるもので、せっかく色々な経験から得た対策や手順がおろそかになります。しかし、現場で高いセキュリティ意識や士気が保持されておれば、このようなことは起こりません。ただし、取扱者の場合、先に述べた経営者やシステム管理者のように自分たちで変えていこうという意識が低いのが通常です。ですから、この意識等を維持させるためには、宣言させるだけではなく刺激を与えることも必要です。その一つの手段が、教育や訓練です。正しい知識を持たせ、問題点や脅威の現状を理解させることにより、全員に危機意識を共有させることが出来ます。もう一つの手段が監査です。現場の人たちとは違った視点で現状を見ることによって、日頃業務に携わっている人たちでは気が付かない問題点や改善点を見つけ出し、業務の適正化を図ることが出来ます。

また、この状態が保持されている職場には、副次的な効果があります。それは、内部犯行の抑止につながるということで、上から下までがセキュリティ確保に真剣に取り組んでいる士気の高い職場においては、不純な動機を持つ人の居場所はありません。もしいたとしても、犯行の機会を作ることは不可能に近

くなります。

5　最後に

組織の中においては、一人で何かをしようとしても難しいことが良くあります。一方で、みんなでやることによって１たす１が２だけではなく、３にも４にもなることがあります。情報セキュリティの分野にも後者のような場合があり、そんなにセキュリティに詳しくない人たちの集まりであったとしても、みんなで協力して活動することにより、それぞれの長所や経験を生かすことが可能となり、思っていた以上の成果を上げることができるようになります。

そもそも情報資産は、活用することでその資産価値が高まります。この認識のない企業等では、「とにかく情報漏えいを起こさない」という消極的な活動にとどまってしまいがちです。現状維持しかできないことは、周りの環境が変化している中においては、相対的に後退でしかありません。常に変化を続けることが、組織を強くして、貴重な情報を保全しつつその資源を最大限に活用するための必要条件です。そのためにも、個人個人がセキュリティに関する意識改革を図り、それぞれが持っている能力を効果的に発揮させる施策が必要です。経営者から現場の取扱者までの一人一人が、セキュリティ確保に対する自己宣言を行い、自分のなすべきことを確実に実施させる環境を作ることにより、それが可能となります。それぞれの立場の人たちが周りの関係者と連携しながら、自分の役割を確実に実行して組織自身を進化させていくことで強固なセキュリティ体制が確立されます。その様な職場環境が作り出されることにより、大切な情報が守られ、それによって情報セキュリティ被害の防止が図れるものだと確信しています。