企業と国に対するサイバー攻撃の実態とその対抗

株式会社ラック　専務理事　西本（にしもと）　逸郎（いつろう）

サイバー攻撃。従前は情報通信技術関係者間での特殊で専門性の高い事象であったが、2010年以降ニュース報道が一般化したと感じる。最近も企業や政府関係機関を狙った攻撃とその被害の報道が後を絶たない。

1．サイバー攻撃とは

現状の危うさを考慮する場合、1995年1月17日に発生した阪神淡路大震災時と2011年3月11日に発生した東日本大震災時の違いを振り返ると理解しやすい。1995年当時、企業における情報通信技術は主に大企業の基幹業務に活用されており、事務所の生産性向上や個人の能力向上の観点での活用度は、それほど高いものではなかった。しかし、東日本大震災においては、一般業務や個人の業務環境が情報通信技術に深く依存していた事実が判明したのは記憶に新しい。この数年間の間に、あっという間、しかも気づかない間に圧倒的に情報通信技術への依存度を高めてしまったのだ。

理由は幾つかある。

1）国際競争力向上のために徹底的な費用削減を求められたこと。大きな削減項目は、具体的には人件費である。そのため、情報通信技術の徹底活用を図ることで、目的を達成した。
2）団塊の世代の引退により、例えば、ものづくりの源泉である彼らの知見などをデジタル化するために、関係するあらゆる業務において情報通信技術を徹底活用するに至った。
3）インターネット、スマートフォン、クラウド、ソフトウェアなどにより私たちの一般業務や生活へ情報通信技術の浸透が重なった。

いずれにせよここ数年の間に、企業の基幹業務だけではなく、様々な活動に必須の情報がデジタル化され、機能はソフトウェア化されたのである。

また、当然のことであるが、何かの目的を持った犯罪者や攻撃者もまた一歩先んじてこの情報通信技術をその基盤とし悪用をしている。特にこの1年ほどで起きたことは、単にインターネットの普及によってサイバー空間が出現し、論理的な壁がなくなったというだけではなく、それまで、海外からの攻撃に対して有効に作用してきた「日本語の壁」も崩壊し、日本のあらゆる層において「開国」がなされた状態になってしまったことも見逃せない。

そのため、様々なサイバー上の脅威を考慮しなければならなくなったのである。

サイバー攻撃とは、このサイバー空間で発生する「事件」を誘発する原因の総称である。実社会と同じように人間が活動し経済が動いている社会である以上、どろぼう、詐欺、業務妨害、風評・風説の流布、産業・軍事・国家などのスパイ活動、社会的な混乱を狙った破壊活動や混乱の誘発、軍事行動などが存在する。

2．サイバー攻撃の実際

実際にどのようなことが発生しているか振り返ってみる。

1）個人情報の流出

多くの組織にとってセキュリティ対策の目的は個人情報の流出対策であることが多い。

例えば、“個人情報流出　お詫び”などのキーワードを入力して検索していただきたい。極めて多くの、事件や事故が発生していることが分かる。単なる誤操作、紛失だけでなく第三者から窃取されたものまで様々である。過失は別として第三者から故意に行われた場合、注意すべきはその「目的・狙い」であるのだが、個人情報に関する事故の場合は、個人情報保護法とその運用に関する各種のガイドラインにより「管理責任」を問われるために、対応手順を優先することになる。結果、例えば営業機密や国家機密と比べ、その手順に従い数多くの情報公開が粛々となされ、多くの事故情報がネット上に存在することになる。しかし、その相手の狙いに言及されていることはまずない。そこは被害企業ではなく、守りきれず「管理が不十分」だった企業としての対応となるため、多くが語られることはない。

ひとつの例を見てみる。例えば、クレジットカードの不正使用が発生した場合、クレジットカード会社側の調査により

どこの加盟店から流出した可能性が高いのかを分析し、当該加盟店に流出有無の調査依頼が入ることが多い。結果、クレジットカード情報以外に個人情報も漏れている（というより、クレジットカード名義も流出するため、一般的には個人情報の流出事件となる）ことが判明し、くだんの個人情報流出のお詫びにつながることが多い。つまり、クレジットカード情報流出と個人情報流出という、二つの事件への対応を個別にやらなければならないことが分かる。

しかし、見逃せない点がある。それは、実はもうひとつの事件が起きていることが多いのである。それは、「不正アクセス禁止法」に関わる事件である。犯人の当該サイトへ侵入した手口のことを想像するかもしれないが、そうではない。こういった事件の多くで「ID、パスワード」（アカウント情報）も同時に窃取されているからである。この場合、取った犯人が不正アクセス禁止法違反となるのはほぼ明白なのだが、実は不正アクセス禁止法ではIDとパスワードへの管理責任も運用者側に問うている、しかし罰則がないため、事実上、運用者側に守らなければならないという意識が希薄である。

つまり、事件はクレジットカード情報流出（割賦販売法）、個人情報流出、アカウント情報流出（不正アクセス禁止法）の三つが起きていることになる。クレジットカード情報を保持していないところで起きる事件ではアカウント情報の窃取が多いが、その場合でも、IDにメールアドレスを使用している場合が多く、メールアドレスは個人情報と捉えることが一般的なため、単に個人情報の流出のお詫びとなるわけである。逆に言えば、個人情報（クレジットカード名義やメールアドレス）の流出がない場合、個人情報の流出とはならず、多くの場合外部に「お詫び」等として公表する義務もないため闇に埋もれてる可能性もあるということである。また、個人情報流出事件として報道されていても、その目的が金銭目的のみと誤解されていることも多い。

クレジットカード情報流出は主にクレジットカード会社の方で積極的に対応しており、利用者側に実害が及ぶことは基本的にはない。個人情報が流出した場合、企業側は隠蔽することが基本的にできないため公表される。が、流出してしまった個人情報に関しては何ら手が打てないし、利用者にとって重要なアカウント情報の流出に関しても特に大きく騒がれることはない。

一方、最近、スマートフォンのアプリを悪用し個人情報を大量に窃取するたぐいのやからへの対抗が厄介であることも話題となっている。

つまり、この観点での課題は3点。

一点目は、流出し、出回ってしまった個人情報を取り戻したり、放棄させるすべがないこと。次に、不正な手口により出回っていると推測される個人情報に自分が関係しているか調べるすべがないこと、最後に、アカウント情報の流出に関して、当人が知る機会がないこと。

もう一点、詳細は後述するが、個人情報の流出は企業の管理責任が問われるという観点で、企業にダメージを与えたいという金銭以外の目的でも窃取される場合がある。

この観点を念頭に入れ責任を負う企業や利用者は対策を考慮することが重要である。

2）業務妨害

例えば「DDoS攻撃 事例」などのキーワードで検索いただきたい。このDDoS攻撃というのは英語のDistributed Denial of Service attackからきている。いわば不特定多数からの業務妨害攻撃である。このDDoS攻撃は世界中で乗っ取られた一般の人のパソコンが攻撃元として使用されることが多い。その乗っ取られた無数のパソコン（「ロ」ボット化したパソコンのネットワーク=ボットネットと呼んでいる）に「攻撃せよ」と命令を送るだけである。世界にはこのボットネットを幾つも構築して、貸し出しする悪徳業者がいるので、そこから借りるのが一般的であるが、場合によっては政治的な目的や主義主張により「みんな」に一斉攻撃を呼びかけ、「みんな」が、能動的に攻撃を行う場合もある。

業務妨害と言えばホームページの改ざんもある。

ここ数年は我が国固有の領土や歴史認識などに関わる行き過ぎた政治的抗議行動から、日本の行政機関や関係機関のホームページが攻撃を受け、閲覧できなくなったり、抗議国と見られる国旗がはためく改ざんが行われたりしている。いわば、サイバー空間での、デモや激しい主張をペンキでなぐり書きするようなものである。

ただし、業務の妨害を目的としなくてもDDoS攻撃やホームページの改ざんは行われる。例えば、金銭目的のために、サイトの業務を妨害し「みかじめ料」を要求したり、その種のウイルスを感染させるために改ざんを行うなどである。つまりは、単に手口と目的は対になっていないことを理解しておこう。

ここで、改ざんに関して少し補足をしておきたい。「たかだか落書き。戻せばいいでしょ」と、多くの方は考えていると思う。

実際に、改ざんが行われるとどうなるか。ある例である。

①バックアップデータから復元する。分かりやすく言うと、落書きをペンキ落としで消すようなものである。犯人は警備をかいくぐって落書きをしたので、当然再度改ざんされることが多い。これを何回か繰り返してしまう。

②改ざんの原因がパスワードの管理や使用しているソフトの脆弱性にあると気づき、それを修復する。しかし、犯人は以前潜入したときに今後のためにバックドアを配置していることも多い。その場合、再度改ざんされることとなる。修正したはずなのにと疑心暗鬼におちいる。外部委託している場合は、信頼関係が揺らいでいるのは間違いない。しかも、バックドアの存在を見つけるのは至難の技。途方にくれることとなる。

③そうこうしているうちに、改ざんされていることが取引先などの知ることになり、「君、うちの情報など漏れてないだろうね。客先にも報告しなければならないので、大至急調査して報告するように。」との連絡が入り、さらに途方にくれることになる。

このようになることは意外に多い。一度、自組織で発生したらどうなるかのインパクトを想定してみるとよい。

ちなみに、当たり前のことであるが、政治的抗議などの主義主張による改ざんで実害を受けるのは、最近は大きなところだけではなく、無名のサイトであることが多い。政府などは、過去から攻撃されていることもあり、改ざんされないように注意喚起し態勢も整えている。一方、攻撃者はペンキを塗れる所から攻めるために、対策の強化が結果として、被害を分散させてしまうことにもなっていると考えられる。その結果、「なぜ、自分のところが」という被害が拡大しているのである。

もう一点、業務妨害を行う側からすると効果的な方法がある。それは、個人情報を流出させることである。前述したように、企業は個人情報流出事件を黙認できない。また、事件当事者に対する世間も厳しく、その管理責任を追及する。その組織をたたき、業務妨害を行うにはうってつけの方法でもあるのだ。

3．サイバー攻撃の目的

どうも、私たちは手口にばかり目がいきがちであるが、攻撃者の目的を考えてみよう。敵を知るのは、原則中の原則である。

「愉快犯」

読んで字のごとくである。あと、自己顕示欲もここに分類してよい。

「主義主張者」

先に紹介した政治的な抗議行動、アノニマス（匿名ハッカー集団と言われている）のような主義主張者、内部告発者、国家や社会への「正義感」の発露などである。

「金銭目的」

先に紹介したような、金銭目的のための情報窃取、詐欺、恐喝など。特に自身の欲のために動く。

「権限拡大」

いわゆる国家レベルのスパイ行為や軍事的行動である。現在のところ、明確な証拠があるわけではないが、そうとしか考えられない事件は多く発生している。

経済や資源などの権益拡大、他国の権益圧ぱくや資源や領土の奪取、及び外交・軍事活動の一環。一般的には国若しくはその関連機関によることが多いと推測されるが、何らかの教義に基づいた組織などによってもたらされることもあると考えられる。また、大規模なインサイダーを仕掛ける、国を代表するような企業の企業価値を奪う若しくは企業そのものを奪うなどの、最終的には金銭目的でも大きな組織によるシナリオと想定されるものは、一般的な金銭目的とは区別し、ここの分類で捉えたほうが整理しやすい。

活動内容としては、標的型の攻撃により組織内に潜入し、システム管理者権限を乗っ取るなどして、長期にわたり情報を筒抜けにできる基盤を整備し諜報活動を行っているものと推測される。また、高度なサイバー兵器の開発や運用も実践していると考えられている。

どんな相手に注意すべきかは、その組織の事業内容や役割により異なる。一般的には国家機関、防衛産業や重要インフラ関連企業が注意すべきであるとの見方も強いが、そうとは限らない。国などを支えるキーマンやキー企業は多く存在するし、本来の狙いに潜入する踏み台として悪用されているかもしれない。

4．どのような手口で行われるのか

様々な手口があるが、スパイ的な活動に関して大雑把に説

明してみる。

1）潜り込む手口

いずれにせよ守られている内部ネットワークに潜り込む必要がある。内部犯あるいは直接潜入した人間がウイルスをコンピュータに感染させる方法もあるが、ここでは、直接こじ開けて入る手口とウイルスを送りつけて感染させる手口の2種類に関して簡単に説明をしておきたい。直接こじ開けてくる手口としてはSQLインジェクションが有名である。ホームページをつかさどるWebサーバの背後にはデータの格納庫であるデータベースサーバが控えていることが多い。インターネット側で稼働しているWebサーバのWebアプリに欠陥があると、SQL（データベースを操作するコマンド）をインジェクション（注入）されてしまい、データベース内の個人情報が盗まれたりするのだ。あと、サーバの設定の不備で容易に侵入されることもよく見かける。

次にウイルスを送りつける方法だが大きく三つの手口がある。一つ目はみんなが集まるWebサイトを改ざんしておき、ここを閲覧したパソコンに強制的にウイルスを感染させるというもの。二つ目は、USBメモリやCDなどを媒体として組織内部に持ち込ませる手口、最後は受信者に開封させる工夫がなされた、標的型メールによる攻撃である。メールに添付あるいは記載されたリンクを巧みに開けさせることで感染させる手口である。多くの場合使用しているパソコン内のブラウザやドキュメント閲覧ソフトのセキュリティ上の欠陥を突きウイルスをインストールされるため、使用ソフトとウイルス対策ソフトを最新にしておくことが唯一無二の対策のように論じられることもあるが、実態はzip内に格納された実行ファイル（EXEファイル）をそのまま実行しているケースも多々見られる。また、最初に狙われた場合、ウイルス対策ソフトが守ってくれることはほとんどあり得ないことも理解しておこう。

2）内部を乗っ取る

金銭目的や愉快犯の場合は侵入することで目的のほとんどを達成しているが、スパイ目的など内部に潜んでありとあらゆる情報を取り続けることのできる環境（私は情報筒抜け基盤と呼んでいる）を構築していくためには、内部ネットワークだけではなく、組織、拠点、役割、使用しているネットワーク、システムの管理方法などを徹底的に調べ上げ、システム管理者の権限を奪い、成りすまして制圧し組織内部を渡っていく。使用されるウイルスはRAT（リモートアクセス型トロイの木馬）がほとんどである。内部に潜入したRATはあらかじめ犯人が用意している外部の指令サーバにあたかもホームページを閲覧する振る舞いで接続し、犯人に自分の情報を伝えるとともに、命令を受け取る仕組みになっている。そのため、この外部への通信が本来のものなのか、潜り込んだネズミ（RAT）が行っているものなのかを見極め選別して止めるような対策方法が必要となり、一般的に「出口対策」と呼ばれている。これまでは、怖いインターネットからの侵入を防げば内部は安全という発想のもと「入口対策」を行ってきたが、これからは侵入されていることを前提にして守っていかなければならない時代になったということである。

ちなみに、内部に情報筒抜け基盤を整備することができれば、やり取りしているメールや閲覧しているホームページや内部に保管している機密文書などいつでも窃取することが可能である。実際の事件でも多くのメールや文書が持ち出されているのは明白であるが、犯人側の厳重な暗号化の措置のため被害実態を100%明らかにできた事例は、私たちがこれまで対応してきた数十件に及ぶスパイ系事件でも1件もない。ちなみに、数十件中、システム管理者権限が奪取されていなかったと確認できたのは僅かに5件のみである。それほど、システム管理者は標的になっているのである。

5．どうすればいいのか

残念ながら、セキュリティ対策に対して明確な動機を持って臨んでいるところは少ない。動機なくして効果的な対策が可能なのだろうか。

その動機を考えるに当たり、情報セキュリティを自動車のブレーキと対比させて考えてみたい。どちらも、進むのに邪魔な存在である。

ブレーキをつけておく理由

例えば「うちの車は下駄」というようなことが昔よく言われていた。近所をはいかい出来れば良いだけでスピードも出ない車。そのため、ぶつかっても大したことはない。下駄にブレーキは要らないのだ。しかし、いくら近所でも公道を走るのであればブレーキはついていないとだめなのである。全くもって無駄なのであるが、叱られるし犯罪にもなる。仕方なくつけておく。現在の情報セキュリティの大半は、正直、このレベルの動機が大半であると感じる。（第一段階）

その後、「下駄」から進歩し移動距離も長くなってくると、「万一のため」という、動機が出てくる。例えると、保険に

加入し、ブレーキもきちんと機能するか確認をしておくこととなる。ところが、これを情報セキュリティに当てはめると、「どこまでやれば良いのでしょうか」という、お馴染みの質問が出てくる。まず、決定的に違うのは「保険」に該当するものは存在しないため、ブレーキはどのくらいの性能が必要なのかという疑問なのだろうが、それは、不毛の議論であると気がつくはずだ。(第二段階)

残念ながら、すごいブレーキを装備し、高価な保険に入っていたとしても最悪の事故は起きてしまうし、そうなると、おじゃんであるということを理解しなければならない。さらに、ブレーキは止めるだけについているわけではない。ましてやてこでも動かなくするだけが目的でもない。もちろんその役割もあるが、重要なことは、最終的に早く移動するためにブレーキは必要なのである。(第三段階)

それは、下駄から、通常の移動手段、さらに事業や生活を支える基盤への進化と、その役割に応じ、ブレーキも役割があるのである。恐らくは情報セキュリティも同様である。情報通信技術をどのレベルで利用しているのかを理解することが肝要である。

もう一点考慮しておきたいのは、情報セキュリティにおける価値観である。分かりやすい例として、「万一のため」と、上記であるが、この「万一」とは何かということである。自組織にとっての万一とは、最悪のケースから列挙してみていただきたい。

これを考える上で、ひとつのヒントがある。私は、生業上、緊急事態が発生した組織に呼ばれその対策を支援することがよくある。その際に気をつけていることがある。ある組織にとっての緊急事態は、その関係者にとっても緊急事態である。当該緊急事態組織の長や従業員の方々が一番気にしているのは、自分たちのことよりも、顧客や利用者たちの、事業継続である。恐らくは、そこが自分たちの事業継続上の肝であることを意識できているからではないかと感じる。

つまりは、まずは「自分のことより人のこと」である。例えば、A社がB社と交渉を行っているときに、A社からB社の情報が第三者に筒抜けになっているとしたら、どうだろうか？　A社自身の情報が漏れている場合と比べ、衝撃は全く異なるものとなる。A社自身の情報が漏れている場合は、ばかにされるか失笑される程度で済むが、他人の情報を漏らしている場合は、信用を全く失ってしまう。A社に対して誰もまじめに交渉はしないだろう。これが、国だったらどうだろうか。力を背景に外交ができる国は別な手段もあるが、そうでない国は、打つ手を失うことだろう。

情報セキュリティにおいて、あれこれやることはあるが、最悪に陥らない手から、少しずつやっていくことが肝要である。

もう一点、考慮すべきことがある。最近はやりの「スマート」である。このスマートとは賢いなどの意味があるようで、その実をあまり理解することができない。ある方がおっしゃっていたが「スマート」というのを「インターネットと融合した」と捉えることで的確に内実を理解できるというのである。

スマートフォン、スマートシティなど、理解できるだろう。そこまで考えると私たちが向かわなければならない先はインターネットと融合した、スマート日本ではないだろうか。社会となったインターネットといかに融合を図っていくか。この、価値観を持つことがまず第一歩である。