業務継続と被害拡大防止を両立させるサイバー攻撃対応

高倉弘喜

皆さん、こんにちは。国立情報学研究所の高倉と申します。私はもともと技術系の人間ですが、今日は、組織が持っているシステムの管理運用に関し、前半ではビジネス面から、後半では技術面からお話ししたいと思います。

一、サイバー攻撃への対応例

⑴ 「インシデント対応＝隔離／遮断」の功罪

我が国では、何か事故が起こった時、組織の持っているシステムをネットワークから切り離すことが当たり前のように行われています。

皆さんの会社のある部門、例えば人事部のパソコンがウィルスに感染した場合、感染被害の広がりがどうか、どのようなデータが漏れたのか全くわからない中で、マスコミの記者やカメラに囲まれて、どうなっているのか、どうするのかと問われます。

その時にすぐに思いつくのが、全社のシステムをネットワークから切り離して対策を検討しているという答えです。これは、対策としてはすっきりしていますが、その結果として、顧客サービス

が止まります。営業機会が失われ売り上げが大幅に減少します。加えて、比較的知られていないのですが、情報インフラが弱体化します。韓国では、わなでサイバー攻撃が行われ、対策を実施しようとしたら、システムが破壊され、データが消滅してしまうような事故が起きています。このようなことにならないよう、正しい手順で対策を講じることが重要です。

三月一六日の朝日新聞で、経済産業省の傘下にある産業技術総合研究所が、ネットワークからシステムを遮断して一ヶ月が経過したと報じられました。今日（四月一〇日）時点でもまだ遮断されたままです。

同研究所はマイクロソフトのクラウドサービスを使っています。そこへのアクセスを許し、ＩＤ、パスワードなどの情報が抜かれてしまいました。マイクロソフトのクラウドサービスには、全所員が使うメール、ドキュメントが置いてあります。重要な研究情報が一気に持ち出される危機に陥ったわけです。経済産業省の指示を受け、同研究所は、二月初旬に全面的にネットワークからシステムを遮断しました。

事実としてはこれだけですが、今これが非常に深刻な事態を引き起こしています。経済産業省からは、一〇〇％の安全を確認することが、ネットワークへの復帰の条件とされています。その結果、一ヶ月が経ってもネットワークに復帰できず、メールやドキュメントを使えない状態が続いています。時間が経てば経つほど、誰も一〇〇％の安全性を保証することはできなくなります。このままでは、いつになってもネットワークへの復帰はできなくなるでしょう。

(2) 日本年金機構の対応（一三〇〇万人分のデータ持ち出し）

三月二〇日、日本年金機構において、一三〇〇万人分のデータが民間事業者の許に持ち出され、その内、五〇〇万人分のデータが中国に渡っていたことが報じられました。

契約によって守秘義務をかけるとしても、一三〇〇万人分の顧客データを外注業者に渡すようなことは通常ではとても考えられません。私どもの研究所でも、いろいろな大学のユーザーのデータを持っておりますが、外注しようとする場合、ダミーデータを業者に提供することはあっても、本物のデータは研究所の中にしか置きません。その上で、業者の従業員に研究所に出向いて作業してもらいます。もしくは、専用の接続窓口を通して、研究所のシステムにアクセスしてもらいます。そうすることで、正しく通信しているか、データを持ち出していないかなどを、研究所が監視できるようにするわけです。

今回の新聞報道を見ますと、契約では八〇〇人で作業することになっていたようです。しかし、実際に業者が使っていたのはたった百数十人でした。厚生労働省の基準では、一人六㎡の作業スペースが必要とされており、八〇〇人では四八〇〇㎡の面積が必要になります。これを家賃に置き換えますと、四ヶ月のスポット契約で一億二〇〇〇万円ほどかかることになります。今回の日本年金機構と業者の契約額は一億八〇〇〇万円でした。そもそもペイするはずがなく、請け負った業者も如何なものかと思います。

契約の内容は、二人組で手入力をするというものでしたが、スキャナで読み取らせた結果を人間が目でチェックしてしまいました。そして、その作業に八〇〇人を充てることになっていました。

請け負った業者は、作業が追いつかなかったために、五〇〇万人分を中国の子会社にやらせました。子会社であったため、委託が禁止されている下請けではないと勝手に判断してしまったものです。結果的に、五〇〇万人分のデータが中国に出てしまうことになりました。

今回のニュースには、もう一つ別の落ちがありました。中国に出した方には全く間違いがないのに、国内で処理した方には多くの誤字脱字があったのです。今や、中国の作業品質は非常に高く、中国の業者は非常によい仕事をしかも安い金額でやってくれます。これは、我が国に対して大変な脅威であると言えます。

（宇治市の教訓）

一九九九年に宇治市で起きた個人情報流出事件から、一つの教訓が得られます。

宇治市役所でアルバイトをしていた大学生が、子育て支援用データを持ち出しました。作業が間に合わないため、市役所の担当者の了解を得て、サンプルデータをフロッピーディスクに入れて持って帰ったものです。その後、この学生は魔が差して名簿屋にフロッピィディスクを持っていきました。

この学生と業者はどのような罪に問えるのでしょうか。学生は、フロッピーディスクのデータを名簿屋に渡しました。しかし、フロッピーディスクはそのまま市役所に返しています。この場合、窃盗罪に問うことはできません。窃盗罪は、電気は例外ですが、財物、つまり形のあるものを盗んだ時しか成立しないためです。

民間企業の場合は、従業員が会社のデータを持って転職しますと、不正競争防止法違反に問うことができます。しかし、宇治市は公的機関であ

り、その業務を妨害する目的でデータを持ち出したわけではありません。このため、この場合、学生についても業者についても、何の罪にも問えないのです。結果的に、裁判では宇治市が負けて、市民に慰謝料を支払うことになりました。

本来であれば、絶対にデータの持ち出しはさせず、渡すとしてもサンプルデータのみとすべきです。どうしても外からアクセスさせる場合も、VPNと言われる専用の回線を使ってアクセスさせるのが原則です。

（データが持ち出された背景）

なぜ日本年金機構は、この教訓を無視して、今回のようなことをしたのでしょうか。その原因は三年前にさかのぼります。

当時、消えた年金問題が起こり、年金がつながらない人（年金保険料を支払ったのに、それに見合った年金の支払いが受けられない人）がたくさん出ました。そこで、このような人の年金をつなぐために、電話窓口を用意し、電話を通じていろいろな条件を聞いて、切れている部分をつなぎ直すサービスが行われるようになりました。

年金をつなぐに当たっては、いろいろな情報を聞いて、名前が間違えて入力されていないかとか、この住所を聞き間違えたらこうなるのではないかなど、いろいろと類推を働かせることになります。しかし、可能性がある全てのパターンを入力して検索するようなことは、ほぼ不可能に近いと言わざるをえません。そこで、このような場合には、一枚のスプレッドシートを用意し、それを人間の目で見て、これとこれがつながっているのではないか、この人が言っているのはこのデータではないかなど、さまざまに推測してつないでいくしかありません。実際にそれをしようと考え

て、つながっていない人の年金データをエクセル表の形で窓口の端末に置いていました。

二〇一五年に機構で個人情報漏えい事故が起きたのはこれが原因です。機構では、この事故への対応として、システムをネットワークから切り離しました。先ほどと同様に、一〇〇％の安全が確認できるまで、ネットワークの利用を制限することにしたわけです。結果的に、機構では、窓口には端末を置かず、窓口と電算室の間の電子データのやり取りも一切行わないことにしました。鉄壁の守りを固めようとして、結果的に、機構が持っている電子データが使えなくなってしまいました。こうした事情が、今回、一三〇〇万人分の個人情報が紙データの形で外部に持ち出された背景にあります。

（二〇一五年の対応の問題点）

三年前の個人情報漏えい事故に対して、日本年金機構はどのような対応をすべきだったのでしょうか。

事故の最終報告書が、一昨年、厚生労働省、内閣官房、サイバーセキュリティーセンター及び機構から出されました。その中で、機構版だけファイルをスキャナで読み取ったような報告書になっています。つまり、機構は、電子データを出せないのです。機構では、今だに外とのやりとりはファックスで行っています。電子データが出せないために、全てが手作業で行われることになっているわけです。

しかし、一〇〇％の安全性を宣言することは誰にもできません。このことは、当たり前と言えば当たり前です。

もし一〇〇％の安全性を確保するためにできることがあるとすれば、パソコン、サーバー、ネッ

トワーク装置、コピー機、プリンターなど、関連する機器を全て新品に入れ替えることです。それによって安全が得られるとしても、データも全て捨てざるをえません。海外では、関連機器を全て入れ替えたのですが、データにマルウェアが取り付いていたため、総入れ替え後、二〇分経ったところで改めて問題が発生したという事例もあります。そもそも、全てのデータを捨てるようなことができるはずがありません。どのように考えても、一〇〇％の安全性は担保できないわけです。

また、一〇〇％の安全性を目指そうとして、外に電子データを出さないことにすれば、その限りでは安全かもしれません。しかし、業務フローを考えないで対策を講じますと、実際に業務を遂行する上で、大穴が空くことになってしまいます。今回、中国に渡ったデータは、確定申告用の年金の支払いデータです。もちろんオリジナルのデータは電子化されておりますが、そのままでは業者に渡すことはできません。電算室から電子データを出してはならないとされているためです。このため、全てのデータを紙に印刷し、業者に渡して、電子化するように依頼したわけです。

しかし、その結果として、民間事業者から情報が漏れるようなことがあれば、元も子もないと言わざるをえません。本当に守らなければならないのは何かを考えて対策を採らなければ意味がありません。

(3) その他の対応例

(自治体の対応)

資料5ページに、一昨年、各自治体で起こった事故への対応を整理しました。日本年金機構の事故の影響が大きく、各自治体の対応は、基本的に機構のやり方を踏襲するものとなっています。例

えば新城市では、消防署の事務部門の二台のパソコンがウィルスに感染しました。それを受けて、同市は、市役所の全業務を三日間止めました。消防署の事務系のパソコンが市役所のネットワークにつながっているためです。

消防署のパソコンでマルウェア感染が見つかったとすれば、それが市役所のパソコンに波及していないかどうか確認しなければなりません。確かにそのとおりですが、確認がとれるまで、市役所の業務を止めなければなりません。その間、住民票も印鑑証明も発行できませんし、通院の給付金の支払いもネットワークへの接続が回復してからになります。

それと同じことが、全国の六つの自治体で相次いで起こりました。基本的に、どの自治体でもネットワークから切り離して対応が行われました。その後、どこも概ね三日で復旧しています。

（ＪＴＢの対応）

次に、民間の対応を見てみます。一昨年、ＪＴＢで情報漏えい事故が起こりました。パソコンがマルウェアに感染して顧客情報が抜けてしまったものです。しかし、ＪＴＢは、サーバーもメールのやりとりも止めませんでした。こうした対応について、マスコミは、日本年金機構の事故対応を知らないのか、システムを全面的に切り離すのが世の中の常識なのに何をしているのか、それほど金を稼ぎたいのかと、厳しくＪＴＢをたたきました。

それでは、なぜＪＴＢはこのような対応をしなければならなかったのでしょうか。理由は簡単です。顧客がいるためです。情報漏えいが起きたのは四月一日でした。調査を行ったのは、四月末から五月初旬の連休中でした。被害の範囲や影響度合いがわからないままで業務を止めますと、連休

明けに全ての状況がわかるまでお客様サポートが止まってしまいます。ゴールデンウィークで旅行中の顧客へのサポートができなくなってしまうわけです。安全に顧客の旅行が継続できるようにするためには、嫌でもシステムを動かさなければなりません。

まだ情報が漏れているかもしれない状況の下でも、業務を続けなければならないわけです。今、日本でサイバー攻撃を受けた時、このような対応はなかなかしづらいところがあります。ＪＴＢの事故の際も、マスコミはＪＴＢをたたきまくりました。国土交通省からもプレッシャーがかかったことでしょう。ＪＴＢがどれほど説明しても理解を得ることは困難です。そのような中で、止めないという判断を押し通すことは非常に大変なことです。しかし、現場でシステムの運用に携わる立場からしますと、ＪＴＢはよく持ちこたえた、よく抵抗したと思いました。

二、サイバー時代の籠城戦の心得

（短期決戦であること）

私は「サイバー時代の籠城戦の心得」と呼んでおりますが、まず重要なことは、短期決戦でなければならないということです。

情報漏えいを阻止するため、システムをネットワークから切り離すことはやむをえないと思います。ただし、切り離しの期間はせいぜい三日以内でなければなりません。それ以上長引きますと、特に企業の場合、巨額の営業収益を失うことになります。つなぎ続けた結果として生じる損失より、システムを切り離したことで儲け損なう金額の方が大きくなるようでは元も子もありません。要するに、営業機会を失うことによる損害額が許

容範囲内に入っているかどうかが問題になります。

（備蓄が十分であること）

次に、備蓄が十分でなければなりません。昔の戦国時代もそうですが、食糧が尽きますと、籠城戦は負けです。要するに、新鮮なデータが存在するかどうかが問題になります。我々が使っているデータは、例えば金融証券系などでは秒単位で使えなくなります。三時間前の株価データを使って取引するとすれば、リスクは非常に大きくなります。ましてや、一週間前の株価で株式を売買するような人はいないでしょう。データの鮮度が非常に短い時間で落ちてしまうわけです。籠城戦をするのはよいのですが、新鮮なデータがなければ負けてしまいます。

（外界からの情報が入手できること）

籠城している間、外からいろいろなデータが持ち込めるようになっていることが重要です。戦国時代の籠城戦では、単に城に立てこもって頑張るだけではなく、城の井戸から城外への抜け道があって、そこを通じて人が出入りしていました。外との連絡を絶って完全に籠城しますと、置かれた状況が何も見えなくなってしまいます。まだ持ちこたえられるのか、降参した方がよいのかを判断するためには、外の情報を入手できることが不可欠です。

（組織内のシステムの弱体化）

今や、セキュリティソフトが分単位で最新のウィルス情報を降らせています。加えまして、マイクロソフトは、原則として月一回セキュリティパッチを配っています。三日間と言えども、その

間に受け取れなかったデータを何らかの形で持ってこないと、システムをネットワークにつなぎ直すようなことは怖くてできません。これが、切り離し期間が長引くほどシステムが弱体化するということに他なりません。三年もネットワークから切り離している期間が続きますと、元の状態に戻すようなことは考えられず、切り離したまま使う戦略しか採れなくなります。

日本年金機構は、三年前に情報漏えい事故が起きた後、ファックスで外からの情報を得ています。しかし、ファックスで新鮮な情報を入手し続けるようなことはほぼ不可能と言わざるをえません。改めてネットワークに復帰できるようにするためには、切り離し期間はせいぜい三日までです。一週間も経過しますと、そのシステムはつながないほうがよいというところまで弱くなります。

（復旧のルールを明らかにしておくこと）

したがいまして、一旦ネットワークから切り離しても、一定期間の内に必ず復帰するというルールを定めておく必要があります。運用ルールでも、セキュリティ対応マニュアルでもよいのですが、このようなルールを書いておかないと、誰も元に戻せないことになります。

一〇〇％安全が確認できた後に復帰するというようなことは、絶対に書いてはいけません。そのような状態は未来永劫来ません。他方、例えば「三日後を目処に安全が確認できたもの」、あるいは「ウィルス感染が確認できなかったもの」は、順次ネットワークに戻して様子を見るといった記述はあった方がよいように思います。このような記述がありますと、それを盾に「手順に従って順次復帰させている」と言えるからです。

なぜこのように申し上げるのかと言いますと、

私どもの研究所も日本年金機構の三日後に事故に遭ったためです。文部科学省からは、至急調査せよとの指示が下りてきました。研究所は、トレンドマイクロとの間で、三営業日以内にウィルスが何物かを明らかにしてもらうという契約を結んでいます。ところが、日本年金機構の事故の三日後で、同社にも余裕がなく、三日たっても回答が返ってきませんでした。我々も専門機関ですので、ざっと見て、広告系のソフトだろうと判断してそのまま放置することになりました。詳しいことは後で申し上げます。

三、サイバー攻撃の実態

マイクロソフトは、年に一度、サイバー攻撃による自社の被害状況についてレポートを出しています。資料８ページには、二〇一六年前半のデータを載せています。これによりますと、マイクロソフトは、全世界の一〇〇以上の国と地域において、六〇万台のコンピューターを持っています。ユーザーは一五万人に上ります。セキュリティ対策は徹底して行われており、アンチウィルスソフトの使用率は九八％となっています。セキュリティソフトが載らないコンピューターを除き、全てセキュリティソフトを載せることを義務付けています。

規模が大きいため、乗っ取り系のウィルスは三四万件、トロイの木馬は三五万件に上ります。トロイの木馬とは、それ自体は悪さをしないのですが、一旦感染しますと、外から仲間を連れてくるようなウィルスです。もう一つ、不要な広告を出すアドウェア系も八〇万件に上っています。

資料９ページに二つの棒グラフを載せています。

左側のグラフは、半年間に、セキュリティソフトが見つけて駆除したマルウェアの件数です。EXEが七八万件、TEMPが三四万件、DLLが二三万件などとなっています。

問題になるのは、右側のグラフです。右のグラフは、例えば朝一番、あるいは夜中にパソコンの中をスキャンした結果、感染したことがわかったマルウェアの件数を表しています。ここで最も多いのが、ワード系のファイルで四五件となっています。一ヶ月では八件程度となります。ここからは読み方なのですが、マイクロソフト全体で一五万人のユーザーがおりますので、一人当たり、月に一個か二個のワード系のマルウェアが来ていると考えてよいと思います。

ここから、一五万人に対して四五件ということであれば、従業員一〇〇人の会社であれば、まずこのようなマルウェアは来ないだろうと受け止める方もおられると思います。しかし、そのように受け止めるのは間違いです。これは、マイクロソフトが装備しているセキュリティソフトをすり抜けられるよう、わざわざオーダーメイドで作られたマルウェアです。ターゲットになると、これぐらいの数が打ち込まれると考えますと、企業のサイズは関係がありません。ターゲットになったら、これだけの数のマルウェアが打ち込まれると考えた方がよいと思います。

今、私は、約一〇〇の国立大学のセキュリティモニターを運用しているセンターの責任者を務めています。そのような立場で見ておりますと、狙われた大学に対し集中してマルウェアがやって来ます。逆に狙われていない大学には全く来ません。ターゲットになりますと、セキュリティソフトが反応しないウィルスが、一ヶ月に八件程度は打ち込まれます。これらのウィルスの感染を防ぐ

ことはできません。

四、サイバー攻撃の態様

（初期潜入後の基盤構築）

サイバー攻撃はメールが送られるところから始まります。メールにはファイルが添付され、それにいろいろなマルウェアが付いてきます。

送られてくるメールは、例えばＪＴＢの場合ですと、航空会社の顧客の搭乗情報をアップデートするといった内容のものです。私どもの研究所の場合は、共同研究者の名前でメールが送られてきます。あるいは、中央官庁の担当者の名前で、「来週の委員会の資料を事前に送付する」といった内容のメールが送られてくることもあります。きれいな日本語で書かれておりますので、もらった方はつい添付ファイルを開いてしまいます。

添付ファイルを開きますと、トロイの木馬系のマルウェアが働いて、別のサーバーにいる仲間のウィルスを呼び込みます。これが第二のウィルスを呼び込み、さらに第三のウィルスを呼び込みます。最後にやってきたこのウィルスが悪さをします。この後、もう一つのウィルスがやって来ます。これは監視ソフトで、先にやってきたウィルスが仕事をしているかどうかを監視します。

なお、以上のステップを全て踏んだところで、第一のウィルスは、トレンドマイクロ、マカフィー、シマンテックなどのセキュリティベンダーに届けられる仕組みになっています。わざわざ作ったウィルスを、一回使っただけで犯人が届けるのです。

実はこれには目的があります。通常、メールを受け取ったターゲットは、「この文書は何か変だ」「この文書は今時来るはずがない」など、何

らかの違和感を持ちます。どのような組織のセキュリティポリシーでも、標的型メールの添付ファイルを開いた場合は、速やかにサイバーセキュリティ責任者に報告することを求めています。しかし、ターゲットとなった従業員は、「報告すると怒られる。始末書を書かされる。ボーナスに響くかもしれない」などと感じがちです。そこでどうしようと思っているところに、一〇分ぐらい経ったところで、セキュリティソフトが「ウィルスを発見したので駆除する」と言ってきてくれるのです。これを見て、従業員は、「ウィルスは駆除されたので、報告はやめておこう」となりがちです。

ところが、第二、第三のウィルスが生き残って動いています。さらに、これらが仕事をしているかどうかを監視するウィルスが付いています。その後、しばらくしますと、第二、第三のウィルスもセキュリティソフトが見つけます。そうしますと、当然これらは削除されます。監視ソフトが、ウィルスが削除されたことを察知しますと、トロイの木馬が働いて、改めて新しいウィルスを呼び込んできます。このため、一回添付ファイルを開いてしまいますと、全てのウィルスを見つけて駆除することはほぼ不可能と言わざるをえません。

私は、添付ファイルを開いたユーザーとの間で、「一〇分後に、改めてセキュリティソフトでスキャンして下さい」「また出てきました」「それでは、三〇分後にもう一度スキャンしてみましょうか」「また出てきました」「先に検査した時に見つからなかったウィルスが三〇分後に検出されるのはおかしいですね」といったやり取りをすることがあります。前に検出されなかったウィルスが三〇分後に検出されるのは、ソフトの切れが悪いためではなく、三〇分前にいなかったウィルスが

トロイの木馬によって新たに呼び込まれたためです。

監視役のウィルスは、乗っ取ったパソコンを手元に置いておくために、ありとあらゆる手を使います。最後に自分自身が駆除されると判断しますと、ディスクを破壊しデータを消していきます。標的型攻撃の犯人は、ターゲットの企業や組織が持っている営業データや特許データを盗みたいのです。しかし、どうしても情報がとれない時には、ライバル会社の持っているデータを消してしまえばよいわけです。そうすることで、ライバル会社を足踏みさせることが可能になります。なお、このようなことは海外では普通に起きていますが、日本ではほとんど起きていません。なぜそうなのかはわからないのですが、非常に不思議な世界です。

（組織内部への侵食）

感染したウィルスは前線基地にとどまらず、そこから徐々に内部に侵食していきます。外の司令サーバーと連絡を取り、次にどこを攻めるかを聞いて、次のコンピューターに攻め込みます。どんどん感染を広げ、機密情報が入っているネットワークのパスを見つけます。パソコンとパソコンの間がネットワークでつながっていないこともありますが、この時も、ＵＳＢメモリーで機密のデータをやり取りしておりますと、ＵＳＢメモリーにウィルスを感染させ、そこにデータを勝手に取り込んで外に持ち出そうとします。

このように、社内に勝手に連絡網を張り巡らせるところまで来ますと、ウィルスを一個駆除しても意味がありません。この場合は、ウィルスを駆除するより、データを守る方が先決です。そのために、システムを隔離することは必要です。この

時、中のデータをどのように外へ持ち出すかは、先ほどの日本年金機構の例のように、紙に印刷するなどの方法が考えられます。なお、その場合も、せいぜい三日程度で何らかの対策を講じなければなりません。

サイバー攻撃を受けて、一つ一つの感染や乗っ取り、つまり個々のインシデント（事案）にあたふたするのはよくありません。逆に、全体を見た時に、これはアクシデント（事態）ではないかと思ったら、アクシデント対応が必要になります。全体を見てどこから手をつけるべきか、何をすべきかという判断が求められます。

ＩＴ専門家は、判断は苦手です。専門家は、「ウィルスに感染している」「外部と通信している」「ＵＳＢメモリーでやりとりが起きている」「ここに機密データがある」といったことは言えます。その上で、「どうすればよいか指示してほしい」と問いかけることになります。その時、「何とかしろ」と言われたら、「どこから手をつければよいか」と問うことになります。

ただ、企業経営上、漏えいしてはまずいデータは何で、それがどこにあるのかについて、ＩＴ専門家が全てを把握しているかと申しますと、それは無理です。他方、経営層が、顧客データがどのサーバーに入っているのかわかっているようなことも普通はありません。ここに、経営層とＩＴ専門家のギャップがあり、その間を橋渡しするものがありません。この点が、今、我が国で最も悩ましいところです。

五、望ましいサイバー攻撃対応

（目的遂行を阻止）

今から八年前、ＩＰＡ（情報処理振興機構）

は、サイバー攻撃を受けて、たとえウィルスの侵入・浸食を許しても、情報を抜かれたり、システムを壊されたりしないような対策を講じるべきであるという考え方を打ち出しました。実はこれは私が主査となり複数の専門家が書いたものです。

三年前に日本年金機構の事故が起こった時、ＩＰＡからガイドラインまで出されているのに、機構はそれを踏まえた対応を行っていなかったとして批判されました。しかし、三年前の時点で機構にそれを求めても無理です。私達がガイドラインを書いた時も、すぐにできるとは思っておらず、早くても一〇年後と考えていました。その後、八年が経っておりますので、そろそろサイバー攻撃への対応に当たっての考え方を変えていかなければなりません。要は、一個一個のインシデントを潰していくのではなく、全体を見て事態をどう収束させるべきかを考える時代になってきています。

（局所的なシステム停止）

万一ウィルス感染が起こったら、被害を受けた部門、例えば人事部のシステムを切り離すのはしようがありません。人事部のデータが経理部に行って給料の支払い事務で使われており、経理部に汚染が広がっている可能性があるようであれば、経理部のシステムの監視を強化することになります。しかし、営業部のシステムはまだ汚染されていないと考えられる状態であれば、そこは通常の業務を継続するという判断をすることになります。

これは、ある部門が被害を受けた場合、被害個所を切り離すことによって、ダメージをコントロールしようとするものです。ダメージの拡大を抑え、生き残った部門は機能を落としながら（こ

れをデグレーデッド・オペレーションと言います）、業務を続けていくような対応が求められています。

このような発想は新しいものではありません。船の運航になぞらえますと、船腹に穴が空こうが、火災になろうが、エンジンが停まろうが、港に帰れる状態である限り、船に乗ったままで帰ってきます。

他方、今、日本で行われているサイバー攻撃対応は、船腹にひっかき傷がついただけで、危険だと言って、全員ゴムボートで脱出するようなものです。まだ船は浮かんでおり、沈むわけでもないのに、太平洋のど真ん中でゴムボートに乗り換えようとするのはかえって危険と言わざるをえません。このようなやり方はそろそろやめなければなりません。船が浮かんでいる間は、船腹に穴が空いても、一生懸命穴を埋めながら、船を動かすという考え方に変えていかなければならないのです。

不思議なことに、ヨーロッパでもそうですが、セキュリティベンダーのマネジャークラスには、三年ほど前まで、空軍出身者がたくさんいて、空軍的なセキュリティ・オペレーションを唱えていました。最近では、空軍出身者に代って、海軍出身者がこのポストを占めるようになりました。海軍出身者が言うのは、ダメージをコントロールしながらビジネスを続けるということです。その本質は、船が沈むまでは、船に乗ったまま、沈まないような方策を講じながら、何とか港に帰ろうとするところにあります。まさにＢＣＰ（業務継続計画）を意識ながら、セキュリティ対応を行おうとする発想です。今はそういう時代になってきています。

（ＣＩＡからＡＩＣへ）

セキュリティの世界では、これまでＣＩＡと言われてきました。

ここで、Ｃ（コンフィデンシャリティー）はデータが外に漏れないこと、Ｉ（インテグリティー）はデータが改ざんされないこと。Ａ（アベイラビリティー）はデータが使えることです。ＣＩＡとは、Ｃが最重要で、それに次ぐのがＩ、最後がＡという考え方です。セキュリティの世界では、日本年金機構の対応に見られるように、コンフィデンシャリティー、すなわち、絶対にデータを漏らさないことが最優先とされてきました。

しかし、ＢＣＰを意識しますと、考え方を変えなければなりません。システムを使って業務ができるのであれば、そのシステムは使えばよいのです。また、一部に不具合があるようなら、後から対策を講じればよいわけです。ＣＩＡからＡＩＣへの転換です。極端なことを言えば、業務を継続することによって、マルウェアに感染してもやむをえないという判断もあり得ます。先ほどのＪＴＢの例のように、感染したウィルスを見つけ切れていない場合でも、旅行中の顧客をサポートするために、業務を継続するという判断もありうると考えられるようになっています。

（エリートパニックによる事態悪化の回避）

セキュリティ対応で最も怖いのはエリートパニックという現象です。

日本年金機構の事故の三日後に、私どもの研究所で広告系のマルウェアが見つかりました。トレンドマイクロに照会し、三日以内に回答するよう依頼しましたが、期限内に回答を得ることはできませんでした。

このような事故が起こりますと、多くの企業

が、全てのファイルをトレンドマイクロに送って、内容の確認を依頼するようになります。添付書類が全て怪しく見えてしまうためです。中には、営業機密の契約書まで送ってくることもあるようです。結果的に、トレンドマイクロはそうした照会への対応に追われ、期限内に私どもの照会への回答ができなかったわけです。

私どもの研究所で調べた結果、送られてきたのはアドウェアであることがわかりました。このことを文部科学省に報告しますと、同省から「それは何か」と問われ、その後、「広告をポップアップで出すソフトだ」「不要な広告は広告と言えるのか」「郵便受けに入るチラシのようなものだ」「チラシの中にはたまに役に立つものがある」といったやり取りをすることになりました。議論がどんどん変な方向に進んでいくわけです。

その結果、文部科学省から、送られてきたマルウェアがどのような物で、どのような機能を持っており、どのようなことをするのか、また、どのようなリスクがあるのかについて、平易な日本語で書いて提出することを求められました。

文部科学省は、私どもが提出した文書を読んでも、内容が理解できず不安になります。本当は重大な事故が起きているのに、それを悟られないために、研究所はいいかげんなことを言っているのではないかと次第に疑心暗鬼になってきます。そこで、文部科学省は、研究所のシステムをネットワークから切り離すように求めてきました。一〇〇%の安全を確保しろというわけです。

そこまで言われて、私は文部科学省に出向き、「冗談ではない」と言って大げんかして、研究所の考え方を押し通しました。しかし、このような対応をするには、相当の覚悟が要ります。私が「ネットワークにつないだままで対策を講じる」

と言いましたところ、文部科学省から「万一のことがあったらどうするのか」と言われました。それに対して、私は「そのようなことがあれば辞める」と言いました。

私の言葉で文部科学省の態度が変わりました。文部科学省も「大したことがないはずなのに、どんどん話が膨らんで大きくなっている」と感じていたのです。しかし、文部科学省の担当者の立場からは、大臣に曖昧な報告はできません。もちろんうそを言うこともできません。そうしますと、誰かが腹をくくって「辞めればよいのだろう」と言わない限り、誰も判断できなくなるわけです。

私がたまたま文部科学省に対応する立場にいて、研究所の立場を押し通していなかったら、私どもの研究所のシステムもいまだにインターネットにつながっていなかったはずです。もしそのようなことになっていたら、「情報学」が専門の研究所がインターネットにつながっていないことが、マスコミで格好の話題にされていたことでしょう。

（経営層とＩＴ専門家の橋渡しの必要性）

システムが攻撃を受けるような事態が生じると、経営層は不安になります。ＩＴ専門家は技術用語しか話しません。経営層の立場からは、技術用語で詳細な説明を受けても、そのようなことはどうでもよいと感じてしまいます。経営層に関心があるのは、サイバー攻撃を受けたことで、会社の経営に影響があるのか、記者会見を行う必要があるのか、顧客に謝らなければならないのか、どの程度の損害につながるのかということでしょう。

他方、ＩＴ専門家は、経営層の関心事には興味がなく、目の前の事象を技術的に説明しようとす

るだけです。したがって、両者はかみ合うわけがないのです。かみ合わなくなりますと、経営層の不安はさらに膨らんでいきます。

私どもの研究所で申しますと、文部科学大臣が先に知ってしまうのが最悪です。このため、文部科学省の人たちが疑心暗鬼に陥らないよう、何が起きたのかについて、できるだけ平易な日本語で書いた資料を文部科学省に提出しました。しかし、技術用語を避けて平易に表現しようとしますと、わけのわからない日本語の文書になってしまいます。結果的に、この文書を受け取った内閣官房から、「文書を読んでも意味がわからないから、技術用語を使った報告を出し直してほしい」と言われることになりました。

このようなことは、海外では普通に起きています。海外では、レポートは、エグゼクティブレポートとテクニカルレポートの二部構成で作成されています。冒頭の三ページから五ページがエグゼクティブレポートです。ここには、何が起きており、それが経営にどの程度の影響を及ぼし、損害額は最大でどの程度かといったことが書かれています。その下に、何が起こったのかについて、技術的に詳細な内容を盛り込んだテクニカルレポートが置かれています。さらに、海外では、これらの二つのレポートが同じことを言ったものであるとの証明書が付いています。

日本では、そのような証明書を付けることになっておりませんので、これがダイジェスト版だと言われても、経営層の立場で、それを信じてよいか不安を持つことになりかねません。ＩＴ専門家の仕事は、そうした経営層の不安を取り除くことですが、それがなかなかできていないのが実情です。昨年、ＦＩＳＣが出した報告書にもありますが、経営層とＩＴ専門家の間で橋渡しをする人

材をこれから育てていかなければなりません。

なお、こうした人材を育てることは、実際には非常に難しいところがあります。と申しますのは、橋渡しする人材は、社外から連れてくることができないためです。ＩＴ専門家であれば、いざとなれば社外から来てもらい、その場で働いてもらうことが可能です。しかし、彼に「会社の経営にどのような影響があるのか」と聞いても、答えられません。彼は、その会社がどのような仕事をしているのか知らないためです。結局、経営層とＩＴ専門家の間のギャップを埋めるのは、外からの助っ人ではなく、社内の人材しかいません。社内で育てなければならず、だからこそ難しいのです。

（コストを意識した対策の必要性）

サイバー攻撃への対策を検討するに当たっては、コストを考慮しなければなりません。

この種の事故が起こりますと、しばしば、特に海外のサイバーセキュリティ会社から「事故を防ぐ製品がある」と言ってきます。実際、そうした機械を購入している大学はたくさんあります。先月も幾つか事故がありましたが、確認しますと、それらの大学の機械は二ヶ月前にウィルスを検知していました。しかし、ウィルスを検知した後の対応がなされていませんでした。機械を買えば、それを運用する人材が必要ですが、多額の費用が必要になるため人材の手配ができていないのです。結局、自分のところで賄える範囲の人材と機械でセキュリティ対応を行っていかなければなりません。

背伸びして高度な機械を入れますと、宝の持ち腐れどころか、事故が発生した時に自分たちに不利な記録が残ることになります。裁判でも、機械

が察知しているにもかかわらず、必要な対策を講じなかったことを認めざるをえなくなります。使いこなせない機械は買わないか、又は、機械の運用を含めて買わなければなりません。この点をよくお考えいただきたいと思います。

（事前のアクシデント対処計画）

何かが起こった時にどのような体制を組むか、予めマニュアル化しておく必要があります。

何があっても止められない業務は、止めない方法を考えておいて下さい。例えば、航空会社は、発券システムが止まりますと、日付、名前、便名を手書きした航空券を渡します。昨年も全日空がそのような対応を行いました。

航空会社の場合、そのようなことができるのは、座席数が決まっているからです。人間の体重はそれほど差がないので、人数を数えることによって、バランスよく積むことができます。人数分だけ手書きで搭乗券を発行し、飛行機に乗り込んだところで前から順番に座席が割り振られます。システムが止まっても、このようなやり方をすれば、手作業で業務を継続することができるわけです。

昨年、日本航空は、システムが止まった時に一日運航を止めました。全日空のシステムが止まり、手書きの搭乗券でしのいだ次の日に、ＪＡＬのシステムが止まったのです。マスコミは、全日空は手書きの搭乗券で飛行機を飛ばしたのに、日本航空は運航を止めてしまった、相変わらずの官業体質でけしからぬという論調で報じました。

しかし、実は、止まった日本航空のシステムは、機体の下部に積むコンテナの重量計算用のものでした。コンテナは一個が一〇トンほどあり、バランスよく機内に積み込まなければなりませ

ん。その上で、飛行機の重心を求め、気温や風速などを入力して、離陸速度を算出するわけです。もしこれを間違えますと、飛行機はうまく飛び上がることができません。その計算を行うコンピューターが壊れたのです。手作業でやることはできますが、一機分の計算で三日かかります。

このため、経営判断として、飛行機を止めるという決断をせざるをえなくなりました。次は、顧客を他の航空会社に振り替えたり、払い戻しを行ったりする方向に運用を切り換えることになります。これは、ＩＴ専門家の仕事ではなく、経営層の仕事です。この点は、マスコミに説明してもなかなかわかってもらえません。発生した問題に対して、どのようにオペレーションを切り換えていくかが非常に重要になってきます。

化学プラントに行きますと、至るところに斧が置いてあります。最悪の事態が生じた場合、この斧で、配管の黄色の×が付いているところをたたき切りますと、プラントは自動停止します。要は壊して止めるわけです。プラントの世界で明治の頃からやっていることを、システムの世界でもやり始めています。工場の世界では、コンピューターがおかしくなった時に、被害を最小限にとどめるため、壊して止めるという考え方もありえます。これからＩｏＴが普及していきますと、私どもの身近なところにいろいろなセンサーや機械が入ってきます。それらがおかしなことをした時には、壊して止めるということも当然選択肢として出てくるでしょう。

六、技術開発の進展

（時間稼ぎによるパニック回避）

以上で申し上げてきたサイバー攻撃対応を全て

人間がやろうとしますと、おそらく破綻してしまうことになるでしょう。ＩＴ専門家も、経営層もパニックに陥りかねません。最初の段階で、ある程度のところまで自動的に機械が対応してくれるようになれば、速やかな対応を求められてパニックに陥ることは避けられるかもしれません。

今、システムがマルウェアに感染した時、自動で当該箇所を切り離し、自動で監視を強化して、「今このような状態で動かしているが、それでよいか」と聞いてくれるシステムの開発が進んでいます。二年から三年後には、これが製品として出てくることになるでしょう。ここではＡＩも活用されることになると思います。

（暫定対策の自動生成）

今や、事故が起こった時に、どのような対策を採ったら、どのような影響があり、どの程度まで被害を抑え込めるかを数値化し、トータルで見て最適な案は何かを示すことができるようになってきています。これを見て、経営層が当座の対策を選んで仮押えし、被害が広がらないような状態を維持したまま、その後の五分から一〇分の間に次の体制を考えることになるわけです。

（米国の動き）

アメリカでは、二年前に、自動でセキュリティホールを見つけ、自動で相手のコンピューターに攻撃をしかけ、さらに、自動で自らを防御するための技を競うコンテストが開催されました。そのような中で、攻撃を受けた時に、この攻撃は危険だと思ったら、自己免疫を作って二発目の攻撃を回避する技術の開発も進められています。かなりＡＩ的な動きと言え、次の作戦を立てて自動で防御をやっていくわけです。最後は人間の判断が

入ってきますが、人間に考える猶予を与える効果を持っています。

また、これは軍事的な側面がありますが、マルウェアに感染したデバイスがどこにあって、どこまで感染が広がっているか、通信をモニターすることによって推定するような研究も進んでいます。

七、まとめ

ここで、以上で申し上げてきたことを整理します。

私どもの社会は情報システムなしには成り立ちません。したがいまして、サイバー攻撃を受け、コンピューターがウィルスに感染したとしても、いきなりシステムを止めるようなことはできなくなっています。

その時、安全を確保しながら、どのようにして業務を継続するかを考えなければなりません。今までのような業務継続か完全遮断の二者択一ではなく、今後は、被害の状況に応じて、部署別に対策に色を付けるようなやり方が必要になってきます。

レジリエンスの考え方も重要です。サイバー攻撃を受けて被害が出るのはしようがありません。一〇〇％の能力は発揮できないにせよ、業務が続けられるのであれば、それでよいという考え方に変えていかなければなりません。

特に重要なのは、被害が出た時にどうするのかを事前に決めておくことです。繰り返しになりますが、運用ルールやセキュリティ対応マニュアルに、「三日経ったら一旦戻すことを考える」という一文を入れておくと有効です。「ここに書いてあるからしようがない」と言えるようにしておく

わけです。この一文がないと、戻そうとした時に、慎重意見を押し切ることが難しくなります。このことは、日本年金機構や産業技術総合研究所の例を見ると明らかです。切り離している期間が長くなりますと、その分被害が大きくなります。産業技術総合研究所の場合、システムを止めてからもう六〇日が経っており、一日数億円の被害が出ています。もしこのようなことを民間企業でやりますと、会社の存続に関わるところまで行ってしまいます。

以上で私のお話を終わらせていただきます。

（拍手）

増井理事長　高倉センター長、どうもありがとうございました。どこでも起こりかねないような、大変具体的なお話を聞かせていただきました。時間が若干オーバーしておりますが、何かご質問はございますか。

それでは、私から質問させていただきます。サイバー攻撃への対応に関しては、今後ともいろいろ対応が必要で、研究も進められていくだろうというお話を伺いました。このようにすれば絶対に大丈夫だという対策が存在するわけではなく、ある意味では非常に恐ろしいという感じも致します。このような状況は、世界で共通なのでしょうか、あるいは、特に日本が遅れているようなところがあるのでしょうか。

高倉　日本でも、政府が個別の事故情報を収集できる制度が整備されました。実務を担う組織も内閣官房に設置されることになっています。問題は、集めた情報をどう精査し、どのように還元するかがまだ決まっていないことです。

二年前のアメリカがまさにそうでした。金融系で情報共有が始まり、一日五〇〇〇件の事故関連

情報が降ってくるようになりました。これだけの情報をさばこうと思いますと、何人の分析者が必要になるでしょうか。大手金融機関では、万単位のセキュリティエンジニアを雇っていると聞いたことがあります。彼らは高給取りですから、このようなことは無駄と言わざるをえません。昨年末頃になって、政府から降ってくる情報を共同で精査する組織を作り、その結果を各金融機関に降らせることになったと聞きました。一日五〇〇〇件の情報と言っても、本当に影響があるのはせいぜい一件か二件です。アメリカでは、昨年からこのような組織がスタートしたわけです。

それと比較しますと、日本は三年から四年遅れています。もっとも、遅れていることによるアドバンテージもあります。日本でも、アメリカの例に倣って、今年又は来年の初め頃には、そのような組織を作る方向に進んでいくのではないかと思っています。日本は、確かに遅れているのですが、それほどひどく遅れているわけではないと思います。

増井理事長　それでは、時間もオーバーしておりますので、この辺りで今日の「資本市場を考える会」を終わらせていただきたいと思います。高倉センター長、どうもありがとうございました。

（拍手）

（**たかくら　ひろき・国立情報学研究所サイバーセキュリティ研究開発センター長**）

（本稿は、平成三〇年四月十日に開催した講演会での講演の要旨を整理したものであり、文責は当研究所にある。）

業務継続と被害拡大防止を両立させるサイバー攻撃対応

高　倉　弘　喜　氏

略　　歴

平成２年九州大学工学部卒、平成４年九州大学大学院工学研究科修士課程修了、平成７年京都大学大学院工学研究科博士後期課程修了。

イリノイ州立大学訪問研究員、奈良先端科学技術大学院大学助手、京都大学講師・准教授、名古屋大学教授などを経て、平成25年国立情報学研究所教授。

平成28年より、同サイバーセキュリティー研究開発センター長