

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たいと思います。

一、サイバー攻撃への対応例

(1) 「インシデント対応Ⅱ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イルスに感染した場合、感染被害の広がりかどうか、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

(二三〇〇万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せんが、外注しようとする場合、データ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向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㎡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ー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、年金がつかない人（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、ほぼ不可能に近く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で、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、窓口と試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うました。こうした事情が、今回、一三〇〇万人分の個人情報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ヤ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くわけです。

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きました。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ぬということです。

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くことが重要です。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つて、そこを通じて人が出入りしていました。外との連絡を絶つ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う。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、外の情報を入手す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イルス情報を降らせています。加えて、マクロソフトは、原則として月一回セキュリティパッチを配っています。三日間と言っても、その

間に受け取れなかったデータを何らかの形で持つてこないと、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、切り離れ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、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らないほうがよいということまで弱くなります。

（復旧のルールを明らかにしておくこと）

したがって、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お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、三日たつ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るように、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、これら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えておりますと、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イルスが、一ヶ月に八件程度は打ち込まれます。これらのウイルスの感染を防ぐ

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イルスを呼び込みます。これが第二のウイルスを呼び込み、さらに第三のウイルスを呼び込みます。最後にやってきたこのウイルスが悪さをします。この後、もう一つのウイルスがやって来ます。これは監視ソフトで、先にやってきたウイ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、第一のウイルスは、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。わざわざ作ったウイルスを、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「ウイルスを発見したので駆除する」と言ってくるのです。これを見て、従業員は、「ウイ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、第三のウイ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イルスが付いています。その後、しばらくしますと、第二、第三のウイルス

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、ウイ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、改めて新しいウイルスを呼び込めます。このため、一回添付ファイルを開いてしましますと、全てのウイ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ようか」「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イ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イ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イルスが

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、次のコンピュータに攻め込みます。どんな感染を広げ、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。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、そこにデータを勝利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、「ウイ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す。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して、そろそろサイバー攻撃への対応に当たった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ら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

れをデグレレード・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)はデータが改ざんされないこと。A(アベイラビリティ)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JT Bの例のように、感染したウイルスを見つけ切れない場合でも、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きます。

(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ったためです。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。もちろんそれ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。経営層に心配があるのは、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。

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ても、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でできないためです。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。社内ですべて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。

（事前のアクセシビリティ対処計画）

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、相変わらずの官僚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

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した。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し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、それでいいか」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、トータルで見ても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。したがって、サイバー攻撃を受け、コンピューターがウイ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ょうがありません。

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有効です。「ここに書いてあるからしょうがない」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行いますと、会社の存続に関わるころまで行ってしまういます。

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す。

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。もつとも、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。)

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研究開発センター長

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
国立情報学研究所

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

「インシデント対応＝隔離/遮断」の功罪

- (標的型?)サイバー攻撃によるマルウェア感染を確認
 - 被害状況(感染台数、感染部署、情報流出の有無)は不明
 - ◆どのような対策が考えられるか?
- 多くの組織で実行されるネットワーク遮断
 - 組織部署、もしくは、組織全体をインターネットから隔離
- これは正しい対応と言えるのか?
 - 業務(顧客サービス)が止まる
 - 営業機会を失う
 - 情報インフラが弱体化する
 - ◆ブービートラップの可能性も
 - 日本では確認されていないが...
- どう対応すればいいのか?

朝日新聞デジタル > 記事

産総研、ネット遮断1カ月

2018年3月16日05時00分

<https://www.asahi.com/articles/DA3S13404765.html>

国立情報学研究所

1,300万人分のデータ持ち出し...500万人分が海外へ

■契約は800人で作業...実態は百数十人

- 800人分の作業スペース...物理的に用意できるか？
 - ◆ 一人当たり最低でも6m²→4,800m²が必要
 - 首都圏だと家賃だけで月額2,000万円台...1.8億円の短期間契約
- 500万人分は中国の子会社へ

■契約で縛っても持ち出す奴は居る

- データは持ち出させない
 - ◆ サンプルはダミーデータ
- VPNでアクセスさせる
 - ◆ アクセス元の制限・把握
 - ◆ 大量データ持ち出しを監視する

■では、なぜこんなことに？

宇治市の個人情報持ち出し事故
(1999年)の教訓はどこに？



<https://www.asahi.com/articles/ASL3M7QSP3MUC1V01M.html>

国立情報学研究所

3

一因は2015年の個人情報流出事件に遡る

■年金機構をインターネットから遮断

- 100%の安全性が確認できるまで
- 端末操作の権限も一部職員に限定
 - ◆ 電話対応職員も端末がない(メモ紙のやりとり)
 - ◆ FAXやUSBメモリでの情報交換



遮断が業務フローに及ぼす
影響を理解していたのか？

■100%の安全宣言を出せるのか？

- 総入れ替えしか手はない
 - ◆ パソコン、サーバ、ネットワーク装置
 - ◆ コピー機、プリンター
 - ◆ データ...と人
- 現実的には不可能
- 3年近く経っても遮断は継続
 - ◆ でも待ってられない業務

業務継続のために却って
セキュリティレベルを下げてないか？

国立情報学研究所

4

それでも続く、数台のマルウェア感染で全業務停止

報道日時	被害組織	感染台数	発端	原因	対応状況
2016年 6月22日	新城市	新城消防署PC2台	不明	不明	市役所を含むネットワーク遮断(6月21日～22日まで)
同日	静岡市	静岡市役所PC1台	警察からの情報提供	不審メールの開封	初期化済み(6月2日) 情報提供後インターネット接続遮断
同日	御前崎市	1台 (他感染可能性のあるPCあり)	警察からの情報提供	不明	マルウェアの駆除、初期化
同日	三豊市	市役所内PC4台	警察からの情報提供	不明	インターネット接続遮断
2016年 6月25日	群馬県	県庁内PC1台	自組織にて検知 外部より情報提供あり	ばらまき型メールの添付ファイル開封	感染詳細の調査中 詳細判明後に公表予定
同日	小山市	小中学校3校のPCがマルウェア感染	警察からの情報提供	構造的メールによると推定	感染したマルウェアは除去済み。 情報漏えいの有無について確認中。

インターネット時代における築城戦

国立情報学研究所

<http://d.hatena.ne.jp/Kango/searchdiary?of=1&word=%2A%5B%A4%A5%F3%A5%B7%A5%7%A5%F3%A5%CB%A4%DE%A4%CB%A4%E1%5D>

5

全業務停止 v.s. サービス継続のジレンマ

■ 2016年に発生したJTB情報漏洩事件

- 3/19-24間に発生した不審通信の発生を一部見逃したのが問題なのか？

発生日	事象	
3/15	攻撃メール着弾	7日間
3/18	起動不能の端末出現・NW隔離	
3/19	委託監視企業よりWebサーバで複数の不審通信の報告・NW隔離と調査	
3/20	調査結果はマルウェア未発見・通信先の一つを遮断	
3/21	サーバでディスク容量不足発生→大容量ファイル確認・業務上不要として削除	
3/24-25	複数の不審通信先を追加遮断・社内端末5台で不正通信失敗を確認	
3/28	端末・サーバでのマルウェア感染を確認→詳細調査開始	
4/1	概要把握→全社CSIRTによる調査開始	
5/13	個人情報漏洩の可能性を認識	業務継続の是非

国立情報学研究所

<http://d.hatena.ne.jp/Kango/20160614/1465925330#20160614f1> より抜粋

6

サイバー時代の籠城戦の心得

- 短期決戦であること
 - 情報漏洩を防止するという観点では正しい
 - 営業機会を失うことによる損害額は許容範囲内か？
- 備蓄が十分であること
 - データの鮮度は→秒単位で賞味期限切れなものも
 - 備蓄が底をつくまでに補充が受けられる見込みはあるのか？
- 外界からの情報が入手できること
 - 営業データ、OS・アプリの更新データ、セキュリティ情報
- 良くて数日...1週間経過すると、組織内のIT系は弱体化する
 - サイバー攻撃の手口は秒単位で進化する
 - 籠城中に適用されるはずだったセキュリティパッチを適用できるか？

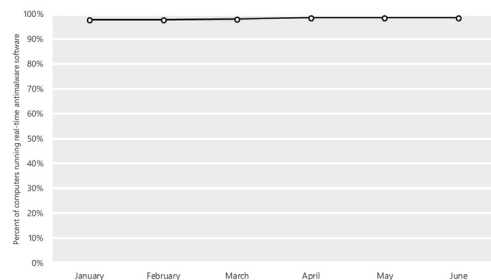
国立情報学研究所

7

万全な対策のマイクロソフトでも...

- 60万台の機器
- 15万人のユーザ
- 100以上の国と地域
- 2016年前半
 - アンチウィルスソフト
 - ◆ 98%以上の使用率
- この規模だと
 - アドウェア系: 80万件
 - トロイの木馬: 35万件
 - エキスプロ系: 34万件

Figure 90. Percentage of computers at Microsoft running real-time antimalware software each month in 1H16



国立情報学研究所

Microsoft Security Intelligence Report Volume 21

8

マルウェア感染を想定した対策の必要性

■ 半年で検知したマルウェア

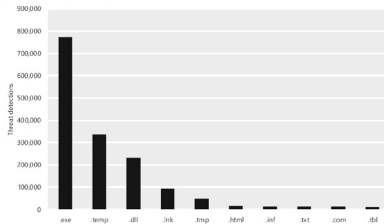
- .exe: 78万
- .temp: 34万
- .dll: 23万

■ 感染後に検知・駆除したマルウェア

- .doc: 45件
- .js: 25件
- .exe: 17件

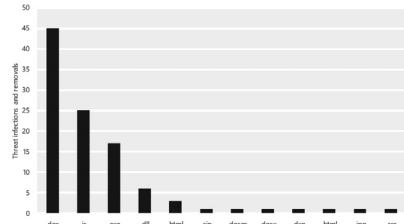
年々増加傾向

Figure 92. Top ten file types used by threats detected at Microsoft in 1H16



国立情報学研究所

Figure 95. Infections and removals at Microsoft in 1H16, by file type



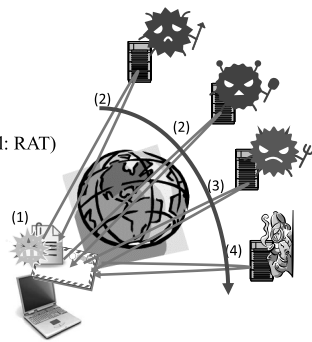
Microsoft Security Intelligence Report Volume 21

9

初期潜入後の基盤構築

■ 誤判断の誘導とステルス化

1. ダウンロード(トロイの木馬)系マルウェア
 - ◆ 感染対象機器の調査...目的のユーザなのか?
 - ◆ 感染後一般公開→駆除成功による誤判断を誘導
2. 多段ダウンロードによる追跡妨害
3. 遠隔操作マルウェア(Remote Administration Tool: RAT)
 - ◆ 組織内部に前線基地を構築
 - 脆弱性探索&攻撃
 - 標的型攻撃メールの素材収集&送信
 - 共有サーバに悪意あるファイル設置
 - 認証サーバ(AD)を攻略
4. バックアッププログラム
 - ◆ RAT駆除等を監視→緊急連絡
 - ◆ オプションとしての破壊活動(サボタージュ)



国立情報学研究所

10

組織内部への侵食

■ 前線基地から徐々に内部へ侵食

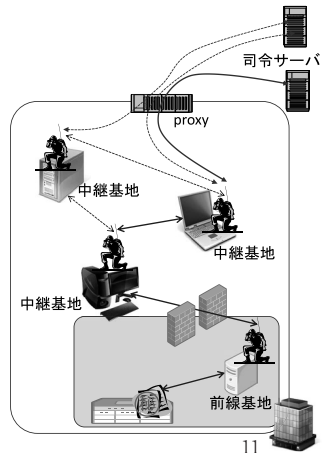
- 前線基地を中継基地化
 - ◆ 外部接続性がない機器と外部との通信を仲介

■ 通信経路の多重化

- 司令サー・中継サーバの多重化
- 組織内に張り巡らされた通信網
- 監視やログ記録を意識した通信手段
 - ◆ セキュリティ製品の検知回避
 - ◆ 目立たない通信
 - 木を隠すには森の中

「記録が見つからない＝被害がない」ではない！

■ 気付いた時にはインシデント(事案)ではなくアクシデント(事態)に



国立情報学研究所

11

高度化する攻撃への対策

■ 従来対策の突破を前提とした対策が必須に

- 従来対策は無用という意味ではない

■ 内部での基盤構築、内部侵入・調査を察知し、目的遂行を阻止

- 内部NWの監視

- ◆ 新たな監視・解析法が必要
- ◆ 追い出してもまた入ってくる



外部(インターネットエリア) ← → 内部ネットワーク

国立情報学研究所

<http://www.ipa.go.jp/security/vuln/newattack.html>

12

レジリエントな情報システムの構築



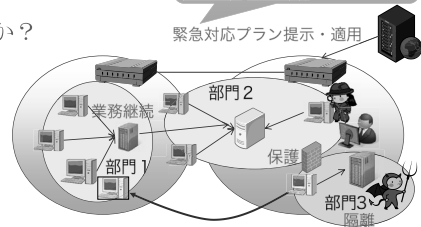
■ 情報システムの全停止は許されない時代に

- 局所的なシステム停止
 - ◆ 被害箇所の切り離し・隔離によるダメージコントロール
 - ◆ 代替措置によるデグレーデッドオペレーション
 - 業務への影響を把握

プランA：部門3隔離
プランB：部門2保護・監視強化
プランC：部門1業務継続

■ 人間がすべての指揮を執るのか？

- 人間系に対する飽和攻撃
 - ◆ パニック状態に陥るのは危険
- 一旦はプランに従って自動対応
 - ◆ 様子を見ながら適宜調整
 - 必要な情報の流れを確保
 - ◆ どこまで自動化できるかを研究



国立情報学研究所

13

CIAからAICへ

■ システム全体が正常に動き続けること (Availability)

- 個々の情報システムの「不具合」が全体のIntegrityに影響するか？
 - ◆ 全体でみた場合、故障とマルウェア感染の区別は無い
 - 不具合は想定範囲内で制御可能なのか？ **ダメージコントロール**
 - 切り離しによる全体への影響は？ **デグレーテッドオペレーションの可能性**

最優先事項

■ 個々の部品から何らかの情報が得られること (Integrity)

- 異常値検知&排除ができるか？
 - ◆ 福岡支店との回線が生きている...も情報

■ 個々のconfidentialityの優先度は一番下

- 極論だが...マルウェア感染しても使えるなら構わない

→レジリエントなシステム設計

単一障害が致命的にならない設計(当たり前の話だが...)

国立情報学研究所

14

エリートパニックによる事態悪化の回避

■エグゼクティブレポートとテクニカルレポートの使い分け

- 「アドウェアって何？」って上司に聞かれたら...
 - ◆「不要な広告表示プログラム」って言い換えれば良いやん！
 - 「不要な広告って広告になるのか？」...ツッコミ入るとそこかい！
 - ・「不要なポステイング広告を表示するプログラム」ならどうだ！
 - ・「不要とはいえ広告をセキュリティソフトが検知するのか？」...



■一段上がるたびに「目黒のサンマ」化する報告書

- 「現場は状況を把握してるのか？」
- 「インシデント対応能力はあるのか？」
 - ◆インシデント対応そっちのけで用語説明書の執筆会議

■どんどん遅れるインシデント対応報告

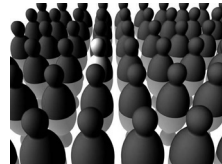
- 軽微なインシデントがアクシデント扱いに

結局、
「意味がわからん。技術用語を使え」
な指示

コストを考慮した対策の必要性

■システム全体を俯瞰する監視体制

- 膨大な情報機器と通信に対する監視
 - ◆平常時：全体をざっくりと俯瞰
 - ◆異常時：異常箇所周辺を精査しつつ俯瞰も継続

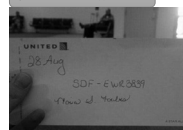


■事前のアクシデント対処計画

- インシデントがシステム全体に及ぼす影響
 - ◆放置すれば深刻な事態に陥るのか？
 - ◆インシデント対応(隔離)がシステム全体に及ぼす影響
 - 何があっても止められない業務の運用継続
 - ◆通信制限、重点監視、代替手段の有無
 - ◆重要セグメントの構築(単独でも業務可能)
- アナログな対応の検討



停止状態の維持...

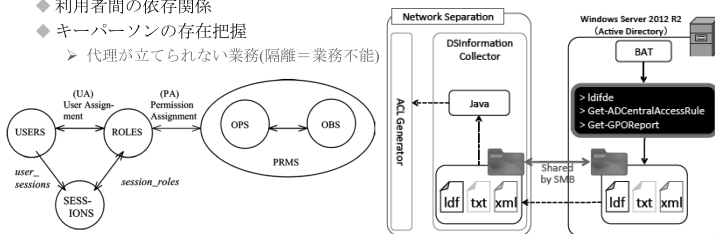


業務フローの把握...PC利用者の情報

- 認証システム(Active Directoryなど)の情報を参照
- ロールベースアクセス制御の登場

- 業務フローの把握

- ◆ 利用者間の依存関係
- ◆ キーパーソンの存在把握
 - 代理が立てられない業務(隔離=業務不能)



国立情報学研究所

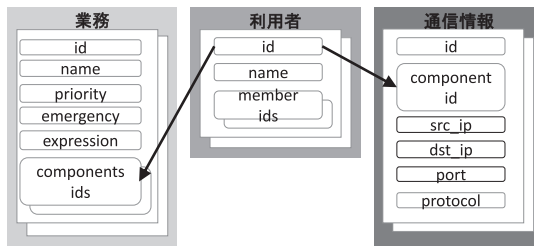
[http://wiki.genexus.jp/hwiki.aspx?Role+Based+Access+Control+\(RBAC%3A+ロールベース+アクセス制御\)](http://wiki.genexus.jp/hwiki.aspx?Role+Based+Access+Control+(RBAC%3A+ロールベース+アクセス制御))

17

業務-利用者-通信との関連性を把握

- 業務を反映したアクセス制御

- 不要な通信を事前に遮断(予防措置、対策案の発散を防止)
- 重要な業務に使用する装置や通信の把握



国立情報学研究所

18

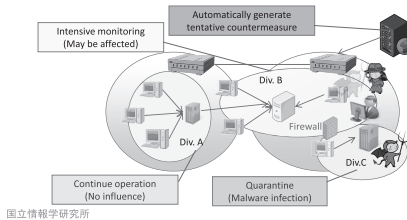
時間稼ぎによるパニック回避

■ 攻撃検知、ネットワーク構成情報等

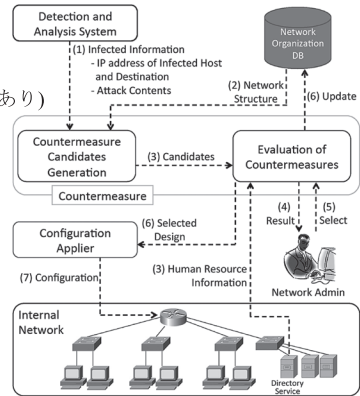
- 複数の暫定対策候補を生成(事前作成もあり)

■ 各候補を評価

- 緩和策による効果
- 運用への影響



国立情報学研究所



19

暫定対策の自動生成

■ 業務フローの情報に基づく

- 対策候補の効果と業務への影響度を数値化
- CSIRTと経営層が連携して最適な案を選択

候補	効果	影響度	総合判定
1. 部門A隔離(業務継続)	1.48	7.0	-0.85
2. サーバセグメント隔離	1.57	11.5	-2.26
3. 感染PC隔離(業務停止)	1.72	1.0	1.39
4. 感染PC遮断(業務継続)	1.87	0.5	1.71
5. サーバ保護	1.84	11.5	-1.99

国立情報学研究所

20

暫定措置の効果と影響の評価

■ 対策適用前後のネットワークの挙動変化を確認

◆ 緩和策の効果

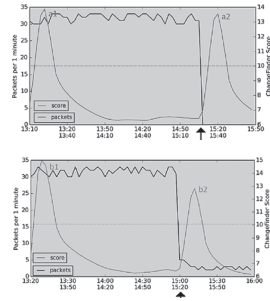
- 攻撃通信を止められているか？
- 不審通信を抑えられているか？

◆ 運用継続への影響

- 正常通信への影響度
- 想定外の正常/不審通信の発生

■ 評価結果に基づく暫定措置の更新

◆ 新たな暫定措置と効果をオペレータに提示



最終的な対策が決まるまでの時間稼ぎ

コネクション番号	送信元IPアドレス	宛先IPアドレス	宛先ポート番号	状態外流量変化
Connection Number	Src IP	Dest IP	Dest Port	
10	192.168.16.1	192.168.30.32	1380	
11	192.168.16.1	192.168.30.31	25	==UNEXPECTED CHANGE==
14	192.168.16.31	192.168.20.3	25	==UNEXPECTED CHANGE==
項目名	暫定措置実施番号	暫定措置変更番号	運用変更番号	関連コネクション番号
Item Name	Temp. Unspecified Change	Temp. Restricted Change	Temp. Change	Related Connection Number
10temp1	[8, 25]	[8, 4]	[8, 25]	[12, 1, 3, 5]
				[12, 4, 5, 6]

国立情報学研究所

21

米国の動き(1)

■ DARPA Cyber Grand Challenge(2016)

- 脆弱性検査(fuzz testing)
 - ◆ 様々なテストデータをプログラムに入力しプログラムを
 - ◆ バグを特定→攻略可能な脆弱性を探索
- パッチプログラムの作成
 - ◆ 見つけた脆弱性に対する暫定パッチを作成する。
- 攻撃プログラムの作成
 - ◆ 他チームのサービスプログラムを停止させる攻撃プログラムを作成
- テストデータによる動作検証
 - ◆ 暫定パッチ適用前後での動作確認

■ これを全て自動化

- 推論エンジンを用いた攻撃開始のタイミング決定
- 解析システム自身のクラッシュ対策

■ DEF CON25 CTF(2017)へ



<https://cgc.darpa.mil>

国立情報学研究所

22

優勝チーム(CMU)でもAIとは言えないのだが...

■推論システムを搭載...一世代前のAI

- 人間が考えたシナリオ
- 様々な条件に基づく動作指示
 - ◆ 脆弱性の可能性を発見
 - 深掘りするか？ 別の脆弱性を探すか？
 - ・ 推定した攻撃のインパクトに基づいて選択
 - ◆ 防御を優先するか？ 攻撃を選択するか？
 - 暫定パッチは副作用の確認などに時間がかかる
 - ・ 相手のシステムを止めた方が高得点だが...
 - 攻撃した瞬間に同じ弾が撃ち込まれるが防御できるか？
 - ・ 気づいていない他チームにヒントを与える可能性
 - ◆ 暫定パッチの動作検証はどうするのか？
 - ◆ 解析システム自体がクラッシュした際の自動復旧

■ これらを全て自動化



国立情報学研究所

23

米国の動き(2)

■ MITRE Challenge IoT

- 不正機器の発見技術
 - ◆ ただし、IoT機器やネットワーク構成には手を入れない
- そのためには...
 - ◆ IoT機器ネットワークの状況把握が必須
 - 攻撃によりIoT機器が乗っ取られた場合に何が起きるのかを予測

■ これって...

- 多種多様な機器環境におけるサイバー攻撃対策
 - ◆ 常に動き回る機器...現在位置を把握できるか？
 - ノートPC、スマートフォン、PDA
 - ◆ サイバー攻撃による被害把握の必要性
 - 物理的な状態から不具合を判断できない

現在は組み込み機器
レベルではあるが...

国立情報学研究所

<https://www.mitre.org/research/mitre-challenge/mitre-challenge-iot>

24

サイバーセキュリティの研究動向(海外)

■ 自己免疫システム

- 未知の脆弱性の発見
 - ◆ セルフチェック
 - ◆ 攻撃手法の解析
- 暫定パッチの開発
 - ◆ IPSを用いた仮想パッチはすでに実用化
 - ◆ 暫定パッチの安全性検証

■ 被害状況に応じた最も効果的な対策を自動生成

- 被害拡大防止&業務への影響を極小化
- ベストの対策ではない可能性はある
 - ◆ 人間のオペレータに考える時間を提供

国立情報学研究所

25

まとめ

■ 情報システムへの依存度増大

- 情報システム抜きに業務はありえない時代に
- 全面遮断による安全確保と業務停止
 - ◆ 二択しかない...という状況からの脱却

■ 攻撃による被害発生を前提とした対策

- 業務継続と被害拡大防止の両立

■ 耐性(レジリエンス)のあるサイバー攻撃対策

- ネットワークの区画化&きめ細かいアクセス制御
 - ◆ ダメージコントロールとデグレーデッドオペレーションによる業務の継続
- 攻撃対策の事前策定
 - ◆ 想定漏れや想定外の副作用の把握
 - ◆ 自動化システムの研究開発
 - ◆ 人間の能力を超えた攻撃への備え

国立情報学研究所

26