企業に求められる「サイバーレジリエンス」

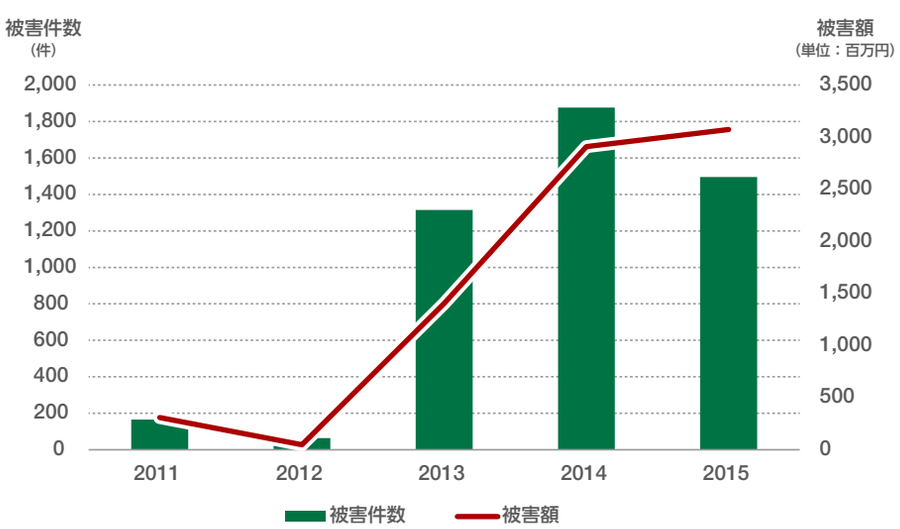
サイバー攻撃後、迅速にビジネスを復旧するには？
適切な対応と回復を重視するサイバーレジリエンス

サイバー攻撃が日常的に発生しており、新聞やテレビで報道されない日はありません。このような状況にあって、サイバーセキュリティーの考え方も、ファイアウォールなどで守りを固めるだけでなく、侵入されることを前提とした対策（出口対策、ログ監視他）の重要性が叫ばれるようになってきました。最近は、この考えをさらに推し進め、攻撃や侵入といったインシデントをあらかじめ想定し、適切な対応によって、被害を最小限に抑え、事業の早期回復を目指す「サイバーレジリエンス」の考え方にも関心が集まっています。

猛威をふるうオンラインバンキング詐欺・DDoS攻撃・ランサムウェア

サイバー攻撃の脅威は、日々増大し続けています。情報処理推進機構（IPA）が発行している「情報セキュリティ白書」の2016年版によれば、2015年のオンラインバンキングを狙った不正送金や攻撃の被害件数は1495件。被害金額は30億7300万円にも上っています。被害件数は前年の1876件より減っているものの、金額は前年比で1億6000万円あまりも増えました。また、攻撃対象も都市銀行や地方銀行だけでなく信用金庫・信用組合へと広がっているのも特徴です。

図1：不正送金の被害の件数と金額



※ IPA「情報セキュリティ白書 2016」をもとに作成

DDoS攻撃は前年比2倍近くに増加しました。こちらは件数だけでなく攻撃トラフィックも10Gbpsを超えるものが全体の20%以上を占めるなど、規模も拡大する傾向がみられます。アノニマスを名乗る、匿名のインターネット活動家の一部は、捕鯨やイルカ漁の反対をアピールするため、自治体や漁協、水族館などを標的に攻撃を展開していますが、取引がある企業や関連する民間企業までもターゲットとして見なされかねません。また主張を広げるため、オリンピックやワールドカップなど、注目を集めるイベントを攻撃対象とすることもあります。ある日突然、DDoS攻撃の被害者になってしまうこともあるのです。

企業に求められる「サイバーレジリエンス」

ランサムウェアの猛威も2016年から続いています。2017年5月にはランサムウェアの「WannaCry」が世界中に被害を及ぼしました。1台が感染すると、脆弱（ぜいじゃく）性を悪用してワームのようにイントラネット内のパソコンに次々と広がっていきます。国内でもメーカーや交通機関など、大手企業の被害が確認されました。

事故が起きない「無謬（むびゅう）性」だけでは乗り切れないサイバー社会

標的型攻撃メール、フィッシングメール、ばらまき型攻撃メールも文面が洗練され、「あやしいメールや添付は開かない」といった注意喚起だけでは、もはや被害を防ぐことはできません。加えてインダストリー4.0やIoT、AIといったトレンドは、これまで以上に、重要なインフラ、製造業、あるいは身近な機器など、さまざまな分野にITが浸透していくことを意味しています。つまりそれは、重要インフラや自動車へのサイバー攻撃、ネットワークカメラのボット化、乗っ取りなどの新たな脅威を生み出す可能性があります。

企業をターゲットにした攻撃メールに添付されるマルウェアは、秒単位で新種・亜種が作られており、従来型のアンチウイルスソフトでは対応が難しい状況です。ログファイルから異常や攻撃を検知しても、すでにマルウェアを実行してしまった後ということも少なくないでしょう。

人々の生活・ビジネスにITが深く関わるほど、技術だけでは守れなくなっているのがサイバーセキュリティーの現状です。

サイバー攻撃が、ビジネス上の被害に直結する時代に

多くの企業にとってサイバー攻撃は無視できない問題となっています。実際にマルウェアに感染して顧客情報や企業の機密情報が漏えいしたり、DDoS攻撃によってサービスが停止すると、どのような被害、損害を受けるのでしょうか。

金銭的被害や業務停止のように被害を定量化しやすいものから見ていきましょう。金融機関がサイバー攻撃を受けて不正送金などをされた場合、その金額がそのまま被害額となります。2016年2月には、バングラデシュ中央銀行がサイバー攻撃を受け8100万ドル（90億円以上）が不正に送金されたという事件も発生しています。

データを暗号化して利用不能にするランサムウェアの被害では、身代金が数万円から数百万円と幅があります。個人所有のパソコンを狙った場合は、個人でも支払いに応じやすくするため3万円前後に設定されることが多いのですが、企業や病院などを狙ったランサムウェアの場合、より大きな金額が要求される可能性があります。また相手は犯罪者であり、泣く泣く身代金の支払いに応じたからといっても、復旧が保証されているわけではありません。金銭をだまし取られた上に、ゼロからデータを再作成するとなれば、膨大な費用が生じる可能性もあります。

DDoS攻撃に関しても、ECサイトなどへユーザーがアクセスできなくなったとしたら、その間、逸失利益が生じます。直接的な売り上げの減少に加え、原因究明や復旧にかかわるコストも発生するでしょう。

サイバー攻撃によって被害が生じたらクライアントやステークホルダーへの説明や対応も必要になります。アカウント情報や個人情報を漏えいすれば、企業は被害者でありながら、ユーザーに補償をしなければなりません。企業ブランドの毀損（きそん）、信用低下による業績への影響といった社会的制裁のほか、行政処分などの対象にもなります。

企業に求められる「サイバーレジリエンス」

経営的な視点で、サイバー攻撃の被害を捉える必要

このような状況において、求められるサイバーセキュリティー対策の考え方で重要なのは、事故の発生を防ぐだけでなく、事故の発生を想定した対応の検討です。

現実問題として、サイバー攻撃による侵入や被害を完全には防げないのなら、攻撃を受けたとき、いかに業務への影響、資産への損害を抑えるかを考えるべきでしょう。

例えば、交通事故であれば、けが人の血を止めることが先決であり、次に2次被害を防ぐための安全確保を行います。「事故を起こしてしまった」「起きてしまった」のであれば、次にやるべきことは、「必要な応急処置を行い、被害をこれ以上悪化させない」ことです。

サイバーセキュリティーでも、攻撃を受けた場合の体制、手順を事前に整えておき、被害を最小限にとどめ、通常業務をなるべく早く復旧させる能力（レジリエンス＝回復力）が問われています。

サイバーレジリエンスの強化には、経営層の理解、関与が不可欠です。不正アクセス、情報漏えいといった事故・事件（インシデント）を起こしてしまったとき、回復が早いほど被害額を抑えることができ、有形・無形の資産を守ることができます。

CSIRTからサイバー保険まで、サイバーレジリエンスに求められる多角的な視点

実際のインシデント対応については、企業内CSIRTといった専門チームを設置することが理想です。CSIRTとは、Computer Security Incident Response Teamの略で、セキュリティーインシデントに対応するための組織です。

攻撃情報の収集、ログの分析、感染PCの解析、外部も含めた関係部署・組織との連携、システム復旧、顧客・ステークホルダー対応など、CSIRTのスタッフはもちろん、情報システム部門に限らず、総務や法務、広報など管理部門を含めたプロフェッショナルの力を結集し、対応します。

中小企業では、CSIRT機能を外部に委託することになりますが、大企業の場合はチームの設置を検討すべきでしょう。CSRITのスタッフは、攻撃情報の収集、各機関との連携、システムの監査・モニタリングだけでなく、従業員の指導・教育などを担当するため、組織全体のセキュリティーを底上げすることにもつながります。

攻撃の予測は非常に難しいですが、標的型攻撃やフィッシングサイト、DDoS攻撃の情報、アノニマスの攻撃予告、トラフィックモニタリングといった情報は、IPA、JPCERT/CC、警察庁といった公共機関の発表はもちろん、セキュリティベンダーなどから得ることができます。

脆弱性情報については、国際的なフレームワークがあり、一定のルールでアドバイザリーやアナウンスが行われています。大手ソフトウェアベンダーやオープンソースコミュニティーもセキュリティーパッチや注意喚起を適宜行っています。

CSIRTなどの体制を整備できていれば、攻撃の予測、少なくとも備えておくことは不可能ではありません。さらに、近年では機械学習やディープラーニングを利用した攻撃の予兆や不正アクセスを検知するソリューションも存在します。

企業に求められる「サイバーレジリエンス」

組織内部の機密情報を狙う標的型攻撃などでは、侵入に気が付かれないよう、攻撃者も慎重に行動します。わずかな兆候を膨大なログから探し出すことは、手間がかかり、困難な作業ですが、AIなどを用いて通常と異なる動きを検出するソリューションも登場しています。

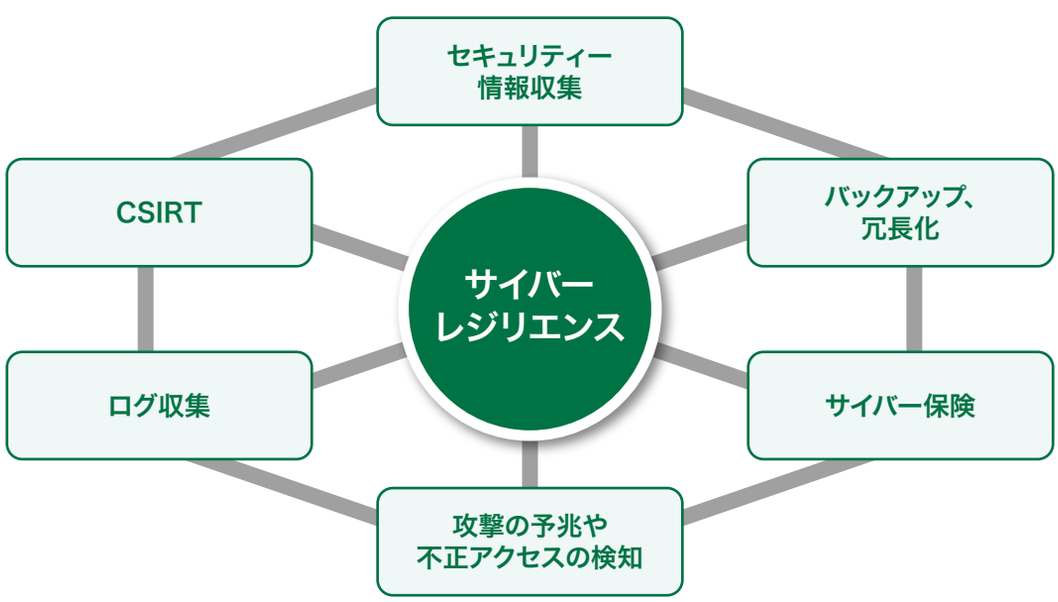
また外部からの防御ばかりだけでなく、バックアップやシステムの冗長化は、インシデント発生後の回復力に大きく貢献します。仮に社内のデータがランサムウェアによって破壊された場合も、バックアップがあればデータを早期に復元できるでしょう。

金銭的被害には、サイバーセキュリティー保険（サイバー保険）も活用できます。サイバー保険は、サイバー攻撃で生じた事故に起因する金銭的な損害を補償するものです。契約にもよりますが、第三者に与えた損害への賠償金や訴訟費用はもちろん、事故調査費用や再作成費用などを補償する商品もあります。サイバー保険を活用することで、キャッシュフローへの影響を極力抑え、大きく膨らむおそれがある賠償費用にも備えることができるなど、経営悪化を防ぐことができます。

巧妙化するサイバー攻撃への「守り」をいくら強化してもリスクはゼロになりません。とはいえ被害の発生を想定し、復旧という視点から対策を講じておくサイバーレジリエンスだけでも被害は防げません。どちらか一方を強化すればよいというものではなく、防御力と回復力のバランスこそが重要となります。

政府が推進する「サイバーセキュリティ経営ガイドライン」では、「サイバーレジリエンス」という単語こそ出てこないものの、事故に備えた対策を求めています。サイバー時代の経営者には、事故が発生するリスクを正しく把握し、その上での経営判断が求められているといっても過言ではないでしょう。

図2：多角的な視点でセキュリティーインシデントに備える



【 制作／コンテンツブレイン 】

NTTコムウェア株式会社
URL：http://www.nttcom.co.jp/
WEB 掲載：2017.9