連載

専門家の 知っ得 解説！

日本技術士会中国本部 活用促進委員会
委員による共著

池田 昌浩
技術士（機械・総合技術監理）

長原 基司
技術士（情報工学・総合技術監理）

正井　慎悟
技術士（経営工学）

Vol.8

サイバーセキュリティ対策とBCP

キーワード　サイバーセキュリティ，サイバーリスク，BCP，フィッシングメール

●当連載について【広島県中小企業団体中央会】

現在、社会変化により、これまで取り組んできたノウハウの蓄積とは異なる分野の技術を必要とするケースが増加していることを感じています。この課題解決のヒントを求め、技術士の方々に当連載をお願いしました。

本件に対する、ご質問・相談は情報調査部にお問い合わせ下さい。（TEL 082-228-0926）

■はじめに

9月8日に広島県中小企業団体中央会主催で開催された「サイバーリスク対策セミナー」に130名以上の参加があったとお伺いし、サイバーセキュリティへの関心の高さに驚きました。これを受け今回は急遽「サイバーセキュリティ対策とBCP※1」と題して特集を組みました。

令和３年度版通信利用動態調査※2によるとクラウドシステムの導入は全企業の70.4%、テレワークの導入は51.9%と高まっており、これがサイバーセキュリティへの関心の高さにつながっていると分析しています。

一方で、IPA(情報処理推進機構)が発行している情報セキュリティ10大脅威2022※3においては、順位の変動はあるもののここ数年上位に来ているのが ランサムウェアによる被害、標的型攻撃による機密情報の窃取、サプライチェーンの弱点を悪用した攻撃、テレワーク等のニューノーマルな働き方を狙った攻撃等となっています。

最近では工場のIT化が進み、生産ラインや生産機器そのもののサイバーセキュリティ対策も重要となってきました。(2010年のシーメンス社製PLC(プログラマブルロジックコントローラ)を狙ったStuxnet(スタックスネット)マルウェア※4事件が有名)

これらのサイバー攻撃の脅威に対して全てに対応することは不可能に近いと言わざるを得ません。そこで、自社のこれらの脅威に対する評価を行い、少ないコストで効率的な対策や攻撃を受けた際のBCPの策定などが重要になってきます。

■サイバーセキュリティ対策3つのポイント

サイバーセキュリティ対策を行う上では、大きく3つのポイントがあります。

a) 情報システムに対する対策

この部分に対する検討ポイントとしては7月号にて著者長原が①データの保全に関するリスク、②システムの稼働に関するリスク、③外部からの不正に対するリスクを挙げその回避とBCPについて触れました。また、この部分に関しては先の動態調査によるとインターネットを利用している企業の98.1%が対策をしていると回答している一方で52.4%の企業が何らかの被害に遭っていると回答しています。

b) 工場などの生産システムに対する対策

生産管理システムやFA機器などは直接ネットワークに接続されていない場合などもありサイバーセキュリティ対策から漏れがちですが、USB機器などを介してのワーム※4感染などもあり、そのリスク評価が必要です。この部分に対しては、経産省が今秋にも工場セキュリティガイドライン※5を発表する予定で、現在の検討経緯が公開されています。

c) サプライチェーンを含めた外部連携に対する対策

最近では電子商取引も一般化しつつあり、これら外部とのデータ交換に潜むリスクなどを評価する必要があります。この部分に対しては、b)のガイドラインに盛り込まれる予定です。

■ネットワークにおける対策の落とし穴

ネットワーク接続システムに対するセキュリティ対策としてセキュリティソフトの導入やセキュリティ対策ソリューションの導入などが一般的ですが、実は中小企業の方々がネットワークに接続する場合、その多くは外部からの攻撃に対しては意外と強いことをご存じでしょうか。現在一般的なプロバイダを経由しての接続には図1に示すNAPT※6と呼ばれるIPアドレス変換技術が採用されており、外部から内部の機器を特定して攻撃することは不可能に近いとされています。

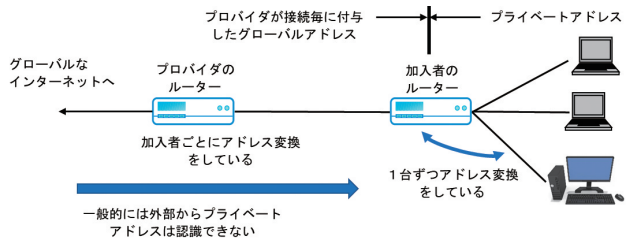

図1 ネットワークシステムのアドレス変換(NAPT)の例

ではなぜ多くのサイバー攻撃事件が起きているのでしょうか。それは「内部から外部にドアを開ける」というワームに感染している、あるいはOSなどのアプリケーションが持つ外部とのバックドア(勝手口)を巧妙に開けるからです。セキュリティソフトの多くは、このワームに感染しないように警告したり、OSなどに存在するバックドアの弱み(セキュリティーホール)の対策を促すなどが主流です。サイバーセキュリティ対策ソリューションにおいてはこれらの攻撃を監視するなどのサービスも提供されています。

そこで重要になるのがソーシャルエンジニアリングへの対策です。これは、あるハッカーが「システムを攻撃するのに高度な技術を駆使するより内部の人間を騙すほうが簡単。」と言っているように、人的なコントロールにより、システムの内部から外部に接続可能とする攻撃方法です。以前は社員に成りすましてID, パスワードを入手する手口が主流でしたが、最近ではスケアウエアのように不安を煽るメールやポップアップ画面で不安を煽ってフィッシングサイトに誘導するなどの手口が多くなっています。このことは、IPAが公表した2021年度中小企業における情報セキュリティ対策に関する実態調査※7の感染経路として最も多いのが「電子メール62.2%」、次いで「インターネット接続(ホームページ閲覧など)45.9%」、「自らダウンロードしたファイル23.4%」からも分かります。

いくら多額の費用をかけても、たった一つのフィッシングメールを開けることによりワームに感染し、それまでの対策を台無しにしてしまいます。

■中小企業で行える具体策～サイバーリスクに備えたBCP～

増え続ける自然災害や新型コロナウイルスの感染拡大により、BCPを策定している企業も増えています。帝国データバンクの2022年調査では、BCPを「策定している」企業は17.7%。企業規模別でみると、大企業は33.7%と伸びている一方、必要性の高い中小企業は14.7%と少なく、課題として、計画策定のスキルやノウハウなどの人材不足があげられています。サイバーリスクに備えたBCPと一般の災害に備えたBCPと何が異なるのでしょうか。

表1に一般災害とサイバーリスクの特徴の違いを示します。

	一般災害	サイバーリスク	対策の特徴
対象	不特定(様々な自然災害など)	標的型が多い	攻撃タイプごとのリスクの洗い出しが必要
当事者意識	被害者	加害者にもなりうる	踏み台にされた場合の加害者としての対策も必要
発災回避	発災回避は困難	対策により発災を回避できる	対策により可能な限り発災を回避することが可能
発災の認知	目に見える場合が多い	困難な場合が多い	発災感知の対策も必要
発災後の対応	自力+行政 原則できるだけ早い復旧	自力のみ 復旧の前に原因究明が必要	該当機器のネットワークからの遮断など急を要するものもある

表1 一般災害とサイバーリスクの比較

この表にもあるように、サイバーリスクは対策により発災を可能な限り少なくすることが可能です。このため、サイバー攻撃に備えたBCPでは、発災後の対策に加えて発災を少なくするための対策も重要となってきます。この中には、データ漏洩に対する対策のように発災後にも重要となる対策もあります。

中小企業のサイバーリスクに対応するための情報セキュリティについてはIPAが中小企業の情報セキュリティ対策ガイドライン※8を公開しており、この中には「5分でできる！情報セキュリティ自社診断」など比較的取り組みやすい内容もありますので、まずは自社診断してみてください。

このIPAの対策と、前述の工場セキュリティガイドラインを組み合わせたBCP策定に着手しましょう。

なにも、高額な機器を買ったり、ITコンサルに頼んだり、使うのが難しいソフトを導入するのがBCPではありません。

日本技術士会中国本部活用促進委員会では、計画策定のスキルやノウハウなどの人材不足に対する技術支援として、これらBCP策定の専門家を紹介する仕組みを構築しています。先ずはご相談ください。

※1:BCP(事業継続計画:Business Continuity Plan):企業がテロ攻撃や災害などの緊急事態に遭遇した際に、事業資産の損害を最小限にとどめつつ、事業の継続あるいは早期復旧を可能とするための事前計画。

※2:令和3年度版通信利用動態調査
https://www.soumu.go.jp/johotsusintokei/statistics/data/220527_1.pdf

※3:情報セキュリティ10大脅威2022
https://www.ipa.go.jp/files/000096258.pdf

※4:マルウェア、ウィルス、ワーム:特定のプログラムに感染するのがウィルス、単独で機能し自己増殖するプログラムをワームと呼び、マルウェアはこれらの総称。自己増殖ではなくメールの添付ファイルの閲覧やホームページの閲覧などで感染する様々な種類のマルウェアもある。

※5:工場セキュリティガイドライン
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/index.html

※6:NAPT(ナプト:Network Address and Port Translation):一つのIPアドレスに対して複数のIPアドレスを割り当てられるように変換する技術。

※7:2021年度中小企業における情報セキュリティ対策に関する実態調査
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

※8:IPAの中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/keihatsu/sme/guideline/