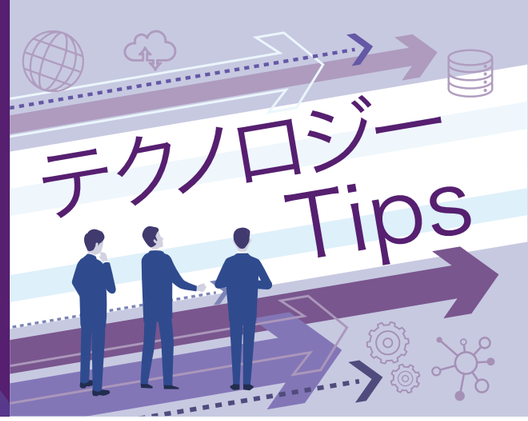
ダイチ通信
今こそ知りたい
＼テクノロジーTips！／
vol.3

DX基盤には必須！

本当に「心配ご無用」？ その「ご無用」こそ心配です……



10つの危険な「心配ご無用」

① パソコンにはワクチンソフトを入れているから心配ご無用

ワクチンソフトは既知のウイルスに対しては有効ですが、新たに作成されたウイルスは検知しません。医療界でも同じことが言えますが、ウイルスの検体がなければワクチンを開発することはできず、どうしても新生ウイルスへの対策は後追いにならざるを得ないのです。ですから、ワクチンソフトを導入しているからと言って安全とは限りません。技術が凄まじい速度で発達していることは攻撃者側も同じです。日々大量のウイルスが作成され、攻撃手法も巧妙化している状況の中で、ユーザー側も常にセキュリティ知識と対策をアップデートしていくことが重要です。

② ウチの社員は怪しいサイトにはアクセスしないから心配ご無用

確かに、明らかに怪しいと分かるサイトにはアクセスしないかもしれませんが、一見すると正規のサイトであっても不正なプログラムが埋め込まれていることがあります。それゆえに、怪しいサイトにアクセスしていなくても被害を受けてしまう場合があるのです。脅威となる攻撃手法を挙げればきりがありませんが、例えば、標的がよく利用するWebサイトを改ざんしてマルウェアに感染させる「水飲み場攻撃」やWebページ上に、リンクやボタンを配置した透明な外部サイトを重ね、外部サイト上で利用者に意図しない操作を行わせる「クリックジャッキング」などがあります。

③ 狙われるのは大きな会社だからウチみたいな中小企業は心配ご無用

大きな会社をターゲットにする場合も、ターゲットと取引関係にあり、セキュリティ対策が弱い中小企業を踏み台にして攻撃が行われることがあります。これを「サプライチェーン攻撃」と呼びます。狙われそうな大会社はセキュリティへの投資も大きく、攻撃者としても直接入り込むことが難しいため、このような手法が用いられるようです。皮肉にも、「ウチは狙われない」などと安穏としている会社ほど、踏み台にされる可能性が高いと言えるのではないでしょうか。踏み台にされる結果、加害者にもなってしまいます。どんな企業でも狙われる危険はあるという認識が必要です。

④ 不正送金被害に遭っても銀行が助けてくれるから心配ご無用

預金者保護法は個人を対象とするもので法人は対象外とされていますが、手口が高度化、巧妙化し、法人の被害も拡大していることを受けて、全国銀行協会は「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方」を発表し法人であっても被害の補償を検討することとしました。ここで重要なのは、法人側もソフトウェアを最新の状態にする等、自らセキュリティ対策を講じ、不正利用被害の防止に努めることが前提となっている点です。いつでも銀行が助けてくれるという他力本願の考えでは、補償を受けることはできません。

⑤ ウチには盗まれて困る情報はないから心配ご無用

盗まれて困る情報を保有していないとしても、先述の通り、セキュリティ対策が不十分だと踏み台にされる可能性があります。つまり、自社に被害がなくても加害者になってしまうかもしれません。セキュリティ対策は自社のためだけのものではないのです。また、攻撃は情報の盗取を目的として行われるとは限りません。例えば、複数のPCを踏み台として、サーバに大量のデータを送り付け、サーバの機能を停止させる「DDoS攻撃」などがあり、大きな被害をもたらします。ですから、盗まれて困る情報がない、というのはセキュリティ対策をしない理由にはならないのです。

⑥ インターネットを使わないという手もあるから心配ご無用

ここまでご紹介してきたリスクがインターネットの利用に起因するものであることから、「だったら、そもそもインターネットを利用しなければノーリスクではないか。」という考えがあるかもしれません。しかしながら、インターネットの利用が当たり前の世の中で、現実味があるセキュリティ対策とは言えません。インターネットは間違いなく社会のインフラであり、事業の運営だけでなく日常生活においてさえ必要不可欠な存在です。また、インターネットに接続しないパソコンであっても USB メモリ等を介して脅威を取り込むことがあるため、ノーリスクではありません。

⑦ サイバー攻撃による被害なんて身近で聞かないから心配ご無用

確かに、メディア等で頻繁に取り上げられる割には、身近なところで被害事例を聞かないということはあるかもしれません。しかし、「聞かない≠被害なし」と考えるべきでしょう。前提として、サイバー攻撃を受けることは好ましくないことです。仮にサイバー攻撃の被害を受けたとして、このマイナスな情報を周囲に言いふらすメリットはありません。むしろ、信用の失墜等、二次的な被害を生じるリスクがあります。ですから、知らないというだけで、身近な会社でも被害を受けていた可能性はあります。サイバー攻撃は架空のものではなく、自社も攻撃されるかもしれないという認識が必要です。

⑧ ウチのパソコンは全部新しいから心配ご無用

サポートが終了したOSを利用しているというのは極めて危険性が高いですが、新しいからと言って安全とは限りません。アップデートをせずに放置していたりすると、結果的に古いOSを使っているのと同様の状況に陥ってしまいます。毎回起動するのが面倒で、何日間もパソコンの電源を入れっぱなし、というケースがありますが、これではアップデートを見逃してしまう可能性があります。使用後に電源を切るという習慣を作り、確実にアップデートを行うことが重要です。

⑨ TLSを使ったサイトしかアクセスしないから心配ご無用

TLS(Transport Layer Security)とは、データを暗号化して送受信するプロトコルの1つで、データの盗み見や改ざんを防ぐとされており、TLSを使ったサイトのURLは「https:// ～」となっています。しかしながら、TLSに対応しているサイトであっても過信するのは危険です。実際、TLSに対応したフィッシングサイトが増加傾向にあると言われており、TLS対応サイトであっても重要な情報が盗取されるリスクがある、という認識は必要です。

⑩ しっかりとID、パスワードを設定しているから心配ご無用

ログイン時などにID、パスワードの入力を要求するサイトも多く、これを設定することには一定の効果がありますが、利用するすべてのサイトで同じIDやパスワードを設定していませんか？1つのサービスから流出したIDとパスワードを他のサービスに流用して不正にログインする「パスワードリスト攻撃」というものがあり、IDやパスワードの使い回しはこういったリスクを増大させてしまいます。できる限り異なるIDとパスワードを設定することをおすすめします。また、大文字／小文字の混用や記号を入れるといった工夫もセキュリティ上有効です。

＼今すぐできる！もう一つのセキュリティ対策！／

体制面の見直しで出来る、もう一つのセキュリティ対策

10コの危険な「ご無用」にしっかりと対策を打ちましょう！
セキュリティ対策は、システムやハードウェア構築が最重要ですが、従業員の意識改革や社内教育、運用・管理体制を見直すことによっても、大きな改善が期待できます。
ここでは体制面での対応策をご提案いたします。

▶ソフトウェアの最新化

ハードウェア以上にソフトウェア、特にOSのアップデートが重要です。
例えば、ワクチンソフトは、先述の通り、既知のウイルスにのみ有効であるという点で、万能ではありませんが、常に最新版へのアップデートを行うことによって、その効果を最大化することは非常に重要です。また、ネットワーク全体で管理すること、ソフトを統一することも効果を高めると言えます。対策ソフトの状況をしっかり把握しておくことです。

▶社内のセキュリティ意識向上

どこに、どんな脅威が潜んでいるか分からない、という危機意識を社内全体で共有する必要があります。外部からの攻撃はもちろんですが、不注意による情報漏えいといった内発的な脅威も重大です。内外の脅威に備えるためにも、セキュリティポリシーの社内外への明示、定期的な社員向けセキュリティ教育を行いましょう。

また、インターネットに接続しないパソコンであってもUSBメモリ等を通して脅威を取り込んでしまう可能性があります。USBメモリの利用や管理についても注意を徹底する必要があります。レガシーシステムには特に注意が必要です。

▶取引先やステークホルダーのセキュリティへの関心

セキュリティが弱い企業を踏み台とする攻撃が激増しています。
取引先や顧客に対して必要以上に懐疑的になる必要はありませんが、取引先のセキュリティ状況をしっかりと把握し、適切な対応を取ることは大切です。
特にお金のやりとりに関わる経理担当者や支払担当者、顧客情報など機密情報をやり取りする人については、まず誰であるかを特定し、明確に確実に管理しておくことが重要です。

▶取扱い情報の明確化

社内には個人情報や社員情報、顧客情報、技術情報など重要な情報が存在しています。
守るべき情報がない、当社の情報なんて狙われるはずがないという考えは大きな間違いです。まずは守るべき情報の特定、管理、そして万が一、情報が漏えいしてしまった場合に、被害・損害を生じるのはどの情報で、どんな被害・損害がどの程度発生するのかを含め、対策をマニュアル化しておくと良いでしょう。
社内の情報管理規定の整備は、法律の観点からも急務と思われます。

▶知識のアップデート

セキュリティの脅威は高度化・多様化しています。ユーザー側もそれに応じてセキュリティのレベルアップを図っていく必要があります。そのためには、サイバー攻撃の最新情報をしっかりと入手し、それを他人事と思わずに適切な対応をとっていくということが非常に重要となります。
当社も、セキュリティに関する最新情報をしっかりご提供します！

＼多層防御とは？／

まずは多層防御とはどのようなものかを確認しましょう。
多層防御とは、情報セキュリティ対策を重ねること。つまり、複数のセキュリティを施してサイバー攻撃の脅威から情報を守ることです。近年ではセキュリティ上の脅威も増え、単一のセキュリティ（例えばアンチウイルスのみ）だけでは対応できなくなっています。

POINT！

多重防御との違いは防御領域の違い！
多層防御と似た言葉の「多重防御」との違いは、防御の領域です。多層防御は入口対策から内部対策、出口対策を複数行います。それに対して多重防御は入口対策のみを重ねて行うことを意味します。

3つの対策領域 ―多層防御の基本的構成―

多層防御の3つの対策領域を見ていきましょう。

1 入口対策　侵入を未然に防ぐ対策

多層防御の入口対策とは、セキュリティ上の脅威を社内ネットワークに侵入させない対策のことです。主な対策は以下の3つです。

① 偽装メールの検知
② Webサイトからのダウンロードの検知
③ スパムメール／疑わしいメールのブロック

2 内部対策　侵入を前提とした拡大対策

内部対策とは、不正アクセスにより脅威となる存在が侵入した後の対策のことです。
実際に社内ネットワークに侵入されたとしても、被害が出る前に食い止められれば問題ありません。また、被害が出てしまった場合も、早急に対処を行えば最小限の被害で抑えることができるでしょう。主な対策は以下の3つです。

① サーバセグメントへの疑わしい通信の検知／遮断とアクセス権の細かい設定
② 疑わしい動作を示す端末の監視と隔離
③ 端末のセキュリティ対策の強化
（エンドポイントセキュリティ・IT資産管理・ソフトウェアアップデート状況）

前述のように、高度な攻撃を仕掛けられた場合には入り口ですべてを防ぐことは困難です。
そのため、上記のような侵入を前提とした対策を行うことで、脅威に素早く気づくことができ、被害を最小限に抑えることができます。

3 出口対策　被害の拡大を防ぐ漏えい対策

出口対策は多層防御の最終ラインであり、侵入後の情報漏えいへの対策のことです。内部対策と同様に、重要な情報を外部に持ち出そうとする動きを検知しブロックします。
主な対策は以下の3つです。

① 疑わしい通信、URLへの通信の検知/遮断
② 操作ログの保存
③ 標的型攻撃対策ソリューション（資産管理・UTM等）の導入

被害の拡大を防ぐためには出口対策が絶対に必要です。

まずは、セキュリティの脆弱性が
どこにあるか診断してみませんか？
まるっと当社にご相談ください！

Daichi SYSTEM 株式会社 ダイチシステム
〒103-0005 東京都中央区日本橋久松町 12-4
TEL：03-5652-9855　FAX：03-5652-9856
E-mail：info@daichisystem.co.jp
URL https://www.daichisystem.co.jp