e-ライフ 新聞
令和5年度 第3版
HPあります！
https://e-lifesogohoken.com

SOMPO 損保ジャパン 代理店
SOMPOひまわり生命 第一生命代理店
e-ライフ総合保険
有限会社江見総合保険
〒700-0823
岡山市北区丸の内2丁目12-20内山下ビル1階
✉：e-lifesogohoken@n1002507.insurance-agt.ne.jp

サイバー攻撃の脅威

昨今、ニュースで取り上げられ、よく耳にする「サイバー攻撃」。
サイバー攻撃とは、インターネット等のネットワークを経由して、パソコンやタブレット等の情報端末に、金銭や個人情報を盗んだりシステムの機能を停止させる目的として攻撃を行うことです。
「マルウェアウイルスにより、某大学から個人情報が〇〇万件流出」「某企業がサイバー攻撃を受け〇〇万件の個人情報が流出」など、耳にしたこともある方が多いはずですが、マルウェアウイルスとは何でしょうか？
サイバー攻撃にはどういう種類があるのでしょうか？

サイバー攻撃を受けた場合、①システムが乗っ取られる ②情報が暗号化される ③金銭を搾取されるといった被害が起こります。

サイバー攻撃は、主に以下の種類があります。

①	マルウェアウイルス攻撃	悪意のあるソフトウェア・プログラムを侵入させ、コンピューターやネットワークに被害を与える攻撃。(例「ウイルス」「ワーム」「トロイの木馬」「スパイウエア」「キーロガー」等)
②	ランサムウェア攻撃	パソコン等に侵入して不正に暗号化したデータを人質にし、復号に身代金を要求する攻撃。最近では暗号化だけではなく、データを窃取した上でそれと引き換えに身代金を要求する手口もある(二重脅迫)
③	パスワードリスト攻撃	何かしらの方法でユーザーIDとパスワードの組み合わせのリストを不正入手し、そのリストに基づいて不正ログインを試みようとする攻撃。ユーザーIDとパスワードの組み合わせリストは、ダークウェブなどで流通している。
④	ブルートフォース攻撃	理論的に考えられるパスワードのパターンすべてを入力するのが「総当たり攻撃」。時間はかかるが、設定したパスワードの文字数が少ないと現実的な時間で突破されることも多い。類似する攻撃として、パスワードに用いられることの多い言葉を優先的に組み合わせて試していく「辞書攻撃」がある。
⑤	標的型攻撃	特定の企業や個人などを狙うサイバー攻撃の手法。ターゲットの情報を調べ上げ、そのターゲットに対して騙せる可能性の高い文面のメールを送り付ける。そのメールに添付されたファイルをうっかり開いてしまうことで、マルウェアに感染してしまい、金銭の詐取、機密情報の漏えいなどの被害につながる。また、秘密裏にマルウェア経由で外部との通信が行われ、感染が拡大するより巧妙な手法もある。
⑥	フィッシング攻撃	大手企業名等を騙ったなりすましメール等を利用して、IDやパスワード、クレジット情報等の重要な情報や金銭をユーザーから詐取することを目的とした手法。

個人に対する攻撃として最近の主流は
①マルウェア攻撃 ②ランサムウェア攻撃 ⑥フィッシング攻撃
が多くみられるそうです。
また最近、Microsoft公式を騙る手口※注1で「警報音が鳴り、PC画面に表示された電話番号に電話したら遠隔操作ができるよう誘導され手数料等を請求されたり、ネットバンキングの送金画面を勝手に操作されたりする」手口や、Amazonや都銀・カード会社などを騙る偽メールから偽の公式サイトに誘導し、カード情報やパスワードを窃取する手口も増えています。
メールを開くときには十分に注意して怪しいメールは開かないようにし、別画面で**公式のHPを開き偽メールの情報等を確認し、公式サイトを見る場合はメール内にあるアドレスからサイトに飛ばず、必ず公式のHPを検索して見ましょう。**
③④の攻撃もある以上、1つのパスワードの使い回しや、誕生日、電話番号、住所等わかりやすいパスワードは控え、大文字・小文字・記号・数字のうち複数種類を使用したパスワードの設定等でセキュリティを高める方法が推奨されています。
※注1： 詳しくは消費者庁のHPへ https://www.caa.go.jp/notice/entry/034736/

承認番号：SJ23-10790
承認日：2023/11/30

企業として、サイバー攻撃への備えは出来ていますか？

サイバー攻撃を受けた場合の被害金額は？

JNSA特定非営利法人日本ネットワークセキュリティ協会は、2017年1月1日から2022年6月30日までの5年半の間に、国内で発生したサイバー攻撃情報を収集し、サイバー攻撃の被害組織（約1,300組織）に対して、2023年7月24日～9月30日までアンケートを実施し、そのうち6%にあたる70件の企業からの回答を得て、以下のような結果を出しています。

被害組織へのアンケート内容	
被害金額	ランサムウェア感染について
被害金額の内訳※	エモテット感染について
対応に要した組織の内部工数（人月ベース）	クレジットカード情報の漏洩について

※被害金額内訳（損害内容）	詳細
• 賠償損害	
• 利益損害	
• 金銭損害	詐欺・脅迫等による被害
• 費用損害	各種事故対応の費用 • 事故原因被害範囲調査費用 ・コンサルティング費用 • 法律相談費用 ・広告宣伝活動費用 • コールセンター費用 ・見舞金や見舞い品購入費用 • ダークウエブ調査費用 ・システム復旧費用 ・再発防止費用
• 行政損害	課徴金、罰金等

結果

被害種別	平均被害金額
● ランサムウェア感染被害※	2,386万円
● エモテット感染被害	1,030万円
● ウェブサイトからの情報漏洩（クレジットカード及び個人情報）	3,843万円
● ウェブサイトからの情報漏洩（個人情報のみ）	2,955万円
● その他のサイバー攻撃被害	473万円

※但しランサムウェアは、各被害にあった組織の多くが被害の影響による機会損失の損害額を算出できていないことと、対応に要する内部工員数が高い傾向にあるため、より大きな損害となる可能性があります。

サイバー攻撃に対する損害費用対策としても有効な「サイバー保険」を当社でも取り扱っております。

サイバー保険の保険料例

試算条件：①支払限度額：賠償1億、費用3,000万 ②自己負担額10万円 ③海外売上高：無
④オプション補償：使用人法令違反復活補償オプション有 ⑤保険期間：1年間
⑥保険料払い込み方法：一括払

事業内容	売上高5億円の場合 保険料例	売上高30億円の場合 保険料例
製造業	65,950円	133,980円
物流業	175,890円	357,280円
建設業	65,960円	133,980円
飲食業	131,920円	267,960円

感染時に被害を少なくするためには、最低限、
定期的なデータのバックアップ（NASの上書き等のバックアップではなく、NAS以外の方法でもバックアップをしておく）、定期的なパスワード更新、WindowsのOSは常に最新版に、ウイルス駆除ソフトのバージョンは更新のお知らせが来たらすぐに更新しましょう！

サイバー保険に関するお問い合わせやご質問等がございましたら、お気軽に担当者までご相談ください。