特集

見えざる脅威から企業を守れ!

インターネットやコンピュータの発展は私たちの生活を豊かにし、企業活動においてもホームページ、メール、電子取引などはすでに必要不可欠なツールとなっている。一方、その発展に合わせて、サイバー空間での犯罪も近年増加している。

誰もがサイバー犯罪の被害に遭う可能性があり、脅威は前触れなく降りかかってくる。もしもの場合に備えた対策や対処法は誰しもが把握する必要がある。

サイバーセキュリティは必須の時代に

ネット社会の進展と共に近年サイバー犯罪が多発している。その被害は個人のみならず企業・団体にも広く及ぶ。

企業にとってのサイバー上の脅威については、IPA（情報処理推進機構）が発表した「情報セキュリティ10大脅威2023（組織）」によると、1位に「ランサムウェアによる被害」、2位に「サプライチェーンの弱点を悪用した攻撃」、3位に「標的型攻撃による機密情報の窃取」が続く。（図表1）

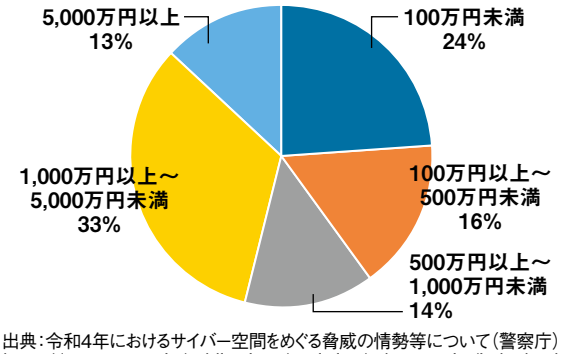
図表1　情報セキュリティ重大脅威2023

1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5位	テレワーク等のニューノーマルな働き方を狙った攻撃
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）

出典：独立行政法人情報処理推進機構　「情報セキュリティ10大脅威2023」
https://www.ipa.go.jp/security/10threats/10threats2023.html

また、サイバー攻撃によりウイルスに感染すると、その被害復旧対応には多大な労力を要する。前述の通り企業への脅威として第1位に挙げられるランサムウェアに関連する被害復旧を見ると、復旧に1週間以上の期間を要したという回答が52%、復旧の費用には100万円以上を要したという回答が76%に及んだ。（図表2）

図表2　調査・復旧費用の総額



出典：令和4年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

こうした被害を防ぐためには日ごろの対策と、被害に遭った際の対応をしっかりと把握しておく必要がある。今回の特集では、企業が被害に遭う可能性があるサイバー犯罪とそれらへの対応について紹介する。

01 INCIDENT

ランサムウェア

ランサムウェアとは

ランサムウェアはマルウェア（悪意のあるソフトウェア）の一種で、Ransom（身代金）とSoftware（ソフトウェア）を組み合わせた造語。パソコンをウイルスに感染させ、そのデータを暗号化して使用を制限し、その解除と引き換えに金銭などを要求する。また、金銭を支払わなければデータを公開すると恐喝する「二重恐喝」と呼ばれる手法が増加している。

感染経路

感染する危険性としては、メールに記載された不正なサイトのURLをクリックしたり、ウイルスに感染した添付ファイルを開いた場合などがある。最近では、VPN機器（※）の欠陥を狙って侵入されるケースも増えている。

※VPNとは…

VPNは、仮想の専用回線を作り、送受信間の通信を暗号化することで、通信の安全性を高める。一方で、アップデートを怠ったり、パスワードを初期設定から変えずにいたところを狙われるケースが増えている。

ランサムウェアによる被害

ランサムウェアの感染により、人質に取られたデータの利用ができなくなり、事業の継続が困難になったり、個人情報が漏洩されるという被害が想定される。

要求された身代金を支払うことでデータが復旧されたという事例もあるが、必ず復旧されるとは言えない。さらには、身代金を支払ったことが却って信用低下につながる可能性もある。もしも被害に遭った場合は、すぐに警察や情報セキュリティ会社への連絡・相談が推奨される。

02 INCIDENT

Emotet（エモテット）

Emotetとは

Emotetはマルウェアの一種であり、メールの添付ファイルを主な感染経路とする。WordやExcelのマクロ機能（作業の自動化に役立つ機能）が悪用され、「コンテンツの有効化」をクリックすることで感染する。感染するとメールアカウントやパスワード、連絡先などの個人情報が窃取される。

ばらまき攻撃と巧妙な手口

Emotetは、感染により窃取したメールアカウントや連絡先などの情報を悪用し、社内や取引先などへ大量のメールを送ることで感染拡大を図る。

盗み取ったメールのやり取りを悪用し、実際のやり取りへの返信などを装うことで、自然に添付ファイルを開かせようとする。

また、ランサムウェアなど他の不正プログラムに感染させる機能も持つため、注意が必要。

03 INCIDENT

内部の不正や不注意による情報漏えい

危険は外部に留まらない

外部からの攻撃だけでなく、社員や関係者、退職者などによる内部の不正、人為的ミスにより、情報等が漏洩する可能性がある。

過去には、退職者が転職活動を有利に働かせるためや、金銭目的のために技術情報などを故意に持ち出した事例、個人情報が入ったUSBを紛失するといった人為的なミスによる事例も発生している。

内部起因による情報漏洩を防ぐためには

内部による情報漏洩は、会社の管理体制が特に問われることになり、企業イメージの悪化や信用問題に大きく関わってくる。

こうした問題への対応としては、社内で使用しているパソコンの台数やソフトウェアを明確に把握すること、情報管理者の明確化、私物のUSBメモリの使用制限、外部へのデータ持ち出しの管理厳格化などが重要となる。

情報セキュリティ意識の向上からサイバー犯罪を防ぐ

ＩＴコーディネータとして県内企業の情報化支援を行うと共に、情報セキュリティマネジメントの枠組みである「ＩＳＯ２７００１」を取得するなど、情報セキュリティ支援に携わる栃川昌文氏に、企業を狙うサイバー犯罪と、その被害を防ぐための取り組みについて伺った。

株式会社ビジネス・アイ　栃川 昌文 氏

企業が被害に遭う可能性が高いサイバー犯罪には「不正侵入」と「ＤＤｏｓ（ディードス）攻撃」の２つがある。

「不正侵入」はメールでウイルスが入った添付ファイルを送るなどして、ネットワークに不正に入り込み、情報の改ざんや個人情報を流出させる。ランサムウェアもその一つであり、不正侵入からウイルスに感染させ、個人情報を人質に金銭などを要求する。

「ＤＤｏｓ攻撃」とは複数のコンピュータからウェブサイトなどに過剰なアクセスを行うことでウェブサイトへのアクセスを遮断させ、事業サービスを停止させるものである。攻撃の狙いは様々だが、社会への混乱や影響を与えることもその背景にある。

これらによる被害を防ぐためには日ごろから対策をとる必要がある。基本的な対策には、最下部に示すような手段がある。

また、対策の中で最も重要なことは、社員のサイバーセキュリティへの意識向上である。不正侵入はウェブサイトやメールを通してウイルスに侵入されることが多く、そういった不審なサイトや添付ファイルを開かないという社員個人の危機意識が第一に重要となる。そのためにも会社としては、世代・役職を問わず社員全体への教育を徹底してほしい。教育の機会も一度きりではなく定期的に実施し、セキュリティ意識を頭に刷り込むことが何よりの対策となる。社員教育にあたっては、ＩＰＡが役立つ動画や情報をまとめたサイトを公開しているので参考としてほしい。

サイバー犯罪は中小企業といえども無縁ではない社会になった。経営リスクの一つと捉え、経営者が先頭に立ち対策を実施していただきたい。

サイバー犯罪の被害を防ぐ基本的な対策

■ウイルス対策ソフトの導入

セキュリティソフトはウイルスの検出や防御を行い、被害を抑えることが期待できる。ウイルスの情報を更新するためにも最新のアップデートを適用する。

■ＯＳアップデートを随時行う

新たなセキュリティの脅威や脆弱性が発見されると随時、その修正が行われている。

■データバックアップをとる

ウイルスに感染した際の復旧を早める。ただし、同じ社内ネットワーク上に保存すると同じくウイルスに感染させられるので、クラウドストレージなどに保存する。

■不審なメールは開かない

添付ファイルにウイルスが仕込まれることが多く、閲覧だけで感染することも。内容も巧妙化しており、身に覚えのないものは開かない。メールを確認する際は一呼吸置いて。

もしもに備えた対応のマニュアル化を

福井県警察本部サイバー犯罪対策課では、日々増加するサイバー犯罪の最前線で、その捜査や広報・啓発活動、対サイバー犯罪への人材育成を行っている。サイバー戦略室長の鶴田勉警視に県内のサイバー犯罪の発生状況や、被害に遭った際の対応について伺った。

福井県警察本部 生活安全部サイバー犯罪対策課
サイバー戦略室長　鶴田 勉 警視

県内におけるサイバー犯罪に関する相談等の件数は下記の通り。昨年は5年前と比較して相談・検挙件数共に増加している。

昨年の相談の内、最も多かった相談は詐欺で943件。サポート詐欺やネットショッピング詐欺などが代表される。次いで不正アクセスによるウイルスなどの被害が406件であった。

	年	件　数
相談件数	2022年	2,142件
	2018年	1,400件
検挙件数	2022年	67件
	2018年	33件

詐欺に関しては、自社の所在地や連絡先が詐欺用の偽サイトに使われるという事例もあった。もし被害者から問い合わせがあれば、内容を確認した上で事情を説明し、双方から警察に連絡するようにしてもらいたい。

ランサムウェアなどのウイルス感染が発覚した場合の対応としては、すぐにLANケーブルを抜くなどして通信を遮断し、被害の拡大を抑えることが重要だ。ここで注意してほしいことは、ルーターやVPN装置の電源を落とさないこと。それらには記録が残っており、その後の調査及び捜査の際に重要となる。同時に被害を確認した時点で、情報セキュリティ会社や警察に連絡をして対応を相談する必要がある。

万が一、サイバー被害に遭った際の備えとして、事前に「インシデントマニュアル」を策定しておくことも効果的だ。予めマニュアルを策定しておくことで被害を最小減に抑えることができると共に、被害からの復旧を早めることも期待できる。マニュアルについては、正しく機能するかの確認も含めて訓練を行い、年1回以上の見直しを行うようにしてほしい。

誰もが被害を受ける可能性を理解することが重要

サイバー犯罪の被害を防ぐには、各個人の情報リテラシーを向上し、危機管理意識を高めることが不可欠である。社内全体で注意点や対応を確認する機会を定期的に設けてほしい。

被害に遭った際の対応については、警察や関係先への報告はもちろん、2022年の法改正によって、情報漏洩が発生した際には個人情報保護委員会への報告も義務化されている。被害の更なる拡大や信用低下を防ぐためにも対応を把握しておくことも重要だ。また、自然災害と同様に、BCP（事業継続計画）や対応マニュアルの策定を業種、規模問わず、あらゆる事業者にお勧めしたい。

福井商工会議所では、IT専門家との相談制度を設けている。自社の情報セキュリティに不安がある方は是非活用して頂きたい。

定例IT無料相談会
毎月第3火曜 13時30分～15時30分
【申込】創業・経営支援課
☎0776(33)8283