8月号 ごあいさつ

セキュリティ対策への備えは万全ですか！？
～ 情報セキュリティを高めるためのサイバーセキュリティ戦略 ～

株式会社 山西　あすなろ会相談役 代表取締役会長　西 垣　洋 一

近年、サイバー攻撃による企業の被害が相次いでいます。ひとたびシステムが停止すれば事業の継続は困難になり、経営に甚大な影響を及ぼします。また情報が流出すれば、信頼の低下や取引停止を招くだけでなく、顧客から賠償を求められ、自社が加害者となるリスクも生じます。サイバー攻撃が巧妙化・多様化する今だからこそ、中小企業においても強い危機感を持ち、事業継続と信頼維持のためのサイバーセキュリティ戦略に取り組むことが必要です。

情報セキュリティだけでない、サイバーセキュリティとの連携を！

情報セキュリティとサイバーセキュリティは似ている概念ですが、中身は異なります。情報セキュリティは「情報そのものの機密性・完全性・可用性を守る考え方全般」、サイバーセキュリティは 「ネットワークや情報システムを通じたサイバー空間上の脅威から情報やシステムを守る取り組み」 を指すことが多く、デジタル化が加速する現代において、企業にとってはどちらも欠かせない重要な取り組みとなっています。

情報セキュリティの概要
- 対象は「情報」全般（紙・口頭・システム内データなど）
- 目的は機密性・完全性・可用性の確保（CIA）
- 組織のルール、物理的対策、人の教育、技術対策を含む

サイバーセキュリティの概要
- 対象はネットワーク・情報システム・IoT 機器などサイバー空間
- マルウェア、不正アクセス、ランサムウェア等への対策が中心

巧妙・多様化するサイバー攻撃と情報資産を守る防衛策

今日のサイバーセキュリティをめぐる状況は、日々刻々と新たなリスクや脅威が発生し、著しく変化しています。また、高度に組織化された情報化社会の中では、Web サイトやブログ、SNS 等の様々なプラットフォームを通して、今この瞬間にも膨大に増え続けています。サイバー攻撃は今や、一部の大企業だけが直面する問題ではなく、生成 AI の普及により攻撃の自動化・精巧化が急速に進み、業種・規模を問わずあらゆる組織がリスクにさらされる時代になりました。

近年の事例を見ても、その手口は年々巧妙さを増しています。生成 AI を悪用した精巧なフィッシング攻撃、身代金を要求するランサムウェアによる事業停止、取引先・委託先を踏み台にするサプライチェーン攻撃、そして公開直後の脆弱性を即座に突くゼロデイ攻撃、これらは今まさに、国内外の企業で被害が続出している現実の脅威です（右図① 参照）。

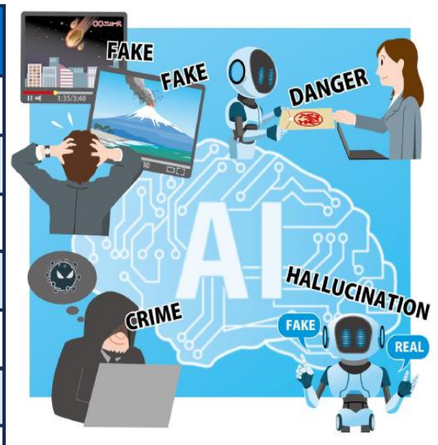
いまや業務にネットワークを使っていない会社はほとんどありません。あらゆる業種がサイバー攻撃のターゲットになりうるものと捉え、情報・サイバーセキュリティ対策を講じることが必要です（右図② 参照）。只残念ながらサイバーセキュリティは「これをやれば完璧」といえる対策は存在しません。新しい手口も次々に登場するなど、どれだけ対策してもリスクがゼロになることはありません。大切なのは、定期的に自社のセキュリティを見直し、「データのバックアップをどうするか」、「システムが復旧するまでどうやって業務を回すか」など攻撃を防げなかったときに備えて BCP（事業継続計画）に組み込むまで準備しておくことが今後の企業経営の責務となります。

当社としても、サイバー攻撃を含めた情報セキュリティの脅威を今一度、重要な経営課題と捉え、自社のセキュリティ対策の高度化と万が一の事態に備えた BCP（事業継続計画）の策定・運用に取り組んでまいります。

2026 年 8 月吉日

（図①）情報セキュリティ 10 大脅威 2026【組織】

順位	「組織」向け脅威
1	ランサム攻撃による被害
2	サプライチェーンや委託先を狙った攻撃
3	ＡＩの利用をめぐるサイバーリスク
4	システムの脆弱性を悪用した攻撃
5	機密情報を狙った標的型攻撃
6	地政学的リスクに起因するサイバー攻撃
7	内部不正による情報漏えい等
8	リモートワーク等の環境や仕組みを狙った攻撃
9	ＤＤｏＳ攻撃（分散型サービス妨害攻撃）
10	ビジネスメール詐欺



出所：独立行政法人情報処理推進機構（IPA）
『情報セキュリティ 10 大脅威 2026』より

（図②）情報セキュリティ６か条

1、 **OSやソフトウェアは常に最新の状態にしよう！**
ＯＳやソフトウェアなどを常に最新版にアップデートしておく。
忘れがちなテレワーク用ＰＣのソフトウェアにも注意が必要。

2、 **ウィルス対策ソフトを導入しよう！**
ウイルス定義ファイルは自動更新されるように設定し、
統合型のセキュリティ対策やウイルス対策のソフト導入を進める。

3、 **パスワードを強化しよう！**
パスワードは１０文字以上で「できるだけ長く複雑に」設定する。
また、多段階認証や多要素認証を利用する。

4、 **共有設定を見直そう！**
ファイルの共有や、ウェブサービス、ネットワーク接続の複合機、
カメラ、ハードディスク（ＮＡＳ）などの共有範囲を限定する。

5、 **バックアップを取ろう！**
パソコンやサーバーに保存したデータも、
こまめにバックアップを取り最新データで保存。

6、 **脅威や攻撃の手口を知ろう！**
ＩＰＡなどのセキュリティ専門機関のサイトで
最新の脅威や注意喚起を確認しておく。

出所：独立行政法人情報処理推進機構（IPA）『中小企業の情報セキュリティ対策ガイドライン第 4.0 版』より