\ここが危ない！/

会社のデジタル化とセキュリティ対策

第1章 中小企業のデジタル化とトラブル対策

第2章 「もの」にまつわる対策

第3章 「おかね」にまつわる対策

第4章 「ひと」にまつわる対策

※本冊子の内容は、令和6 年11 月1 日現在の法令等にもとづいています。

第2節 デジタル化とトラブル対策は同時に行う

企業が認識するべきセキュリティリスク

企業がデジタル化を推し進めていく上で認識しなければならないのが、セキュリティリスクです。情報セキュリティ対策を怠ると、以下のような不利益を覚悟しなければなりません。

金銭の喪失	個人情報や機密情報の紛失は、多額の損害賠償請求のリスクがあります。また、不正送金やカードの不正利用の可能性もあります。
顧客の喪失	セキュリティ事故により企業の社会的評価が低下し、受注停止や安全な取引先への変更など、顧客離れが懸念されます。
事業の停止	パソコンやシステムが利用不能になり、長期にわたり仕事ができないだけでなく、生産の停止や取引先への影響が長期にわたり続く可能性があります。
従業員の離反	従業員が働く意欲を失い、従業員のモラルの低下や、情報漏洩などの事故による企業としてのイメージダウンにより従業員が離職したりするリスクがあります。

たった一度のセキュリティ事故の発生により、中小企業は事業の存続が危ぶまれ廃業に追い込まれることもあります。中小企業のセキュリティ対策は、デジタル化によって高まるリスクを経営者が理解し、経営者が主導して進めていくことが求められるといえるでしょう。

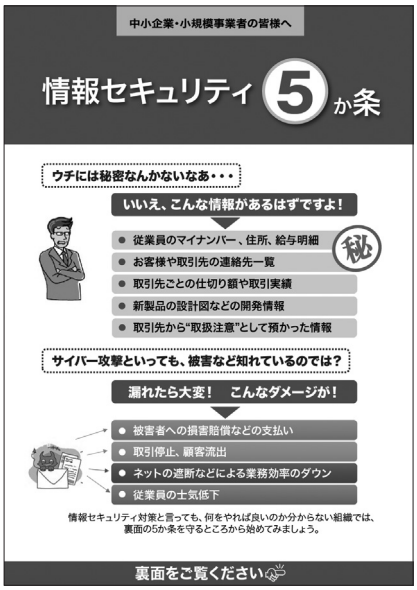
デジタル化とセキュリティ対策は表裏一体

デジタル化だけを進めてセキュリティ対策が後手に回ってしまうと、デジタル化した情報資産は、情報漏洩のリスクにさらされます。デジタル化したデータを取り扱う従業員のセキュリティ教育がなされていないと、人的ミスや内部犯行が常態化するかもしれません。

セキュリティリスクが増大する現在において、情報セキュリティ対策なくしてデジタル化を進めることは極めて危険です。情報セキュリティ対策があってこそ、デジタル化の恩恵を最大限に受けることができるのです。

中小企業のセキュリティ対策の最初の一歩

それでは、中小企業のセキュリティ対策は、どのようなことから始めればよいのでしょうか。一般的には、セキュリティ対策にはそれなりの投資が必要と考えられています。たしかにお金がかかる対策もありますが、基礎的なセキュリティ対策はほとんどの場合、無料で対応できます。独立行政法人情報処理推進機構（IPA）が公開している情報セキュリティ５か条を参考にして、基礎的な対策をしっかりと行うことから始めましょう。



情報セキュリティ5か条

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

出展：独立行政法人情報処理推進機構HP「中小企業の情報セキュリティ対策ガイドライン」付録1：情報セキュリティ５か条

自社の状況を正しく把握して具体的なセキュリティ対策を

情報セキュリティ５か条への対策だけでは、十分な対応であるとはいえません。そこで、次のステップとして同じIPAが提供している「５分でできる！情報セキュリティ自社診断」を利用しましょう。

これを利用することで、自社の情報セキュリティ対策の現状を簡単に評価することができます。具体的には、基本的なセキュリティ項目に関する質問に答えることで、セキュリティの強化が必要な領域を特定し、対策の優先順位を把握することができるのです。また、診断結果に基づいて具体的な改善策や対策ガイドラインが提供されるため、迅速かつ効果的なセキュリティ強化が実現できるといえるでしょう。

第2章 「もの」にまつわる対策

第1節 情報機器のセキュリティ対策

情報機器ごとに認識すべきセキュリティリスク

IoT*の進展や業務の多様化により、私たちが利用する情報機器も多様化しています。情報機器ごとに認識すべきセキュリティリスクは以下のとおりです。

＊アイオーティー（Internet of Things）：現実の様々なモノが、インターネットと繋がること

パソコン	業務に最も利用される情報機器です。利用頻度が高く、攻撃対象になりやすいといえるでしょう。マルウェア*などを利用して、業務用のパソコンを踏み台に企業のネットワークに侵入されるリスクがあります。従業員が意図せず不正なサイトにアクセスしてしまったり、紛失や盗難でハードディスクの情報が漏洩したりするリスクもあります。
スマホ タブレット	気軽に利用できるスマホやタブレットは、業務用としてはビジネスチャットやクラウドサービスへのアクセスに利用されています。このため、ビジネスチャットを通じた情報漏洩や、クラウドサービスへの不正アクセスのリスクがあります。紛失や盗難を通じた情報漏洩にも注意が必要です。
ウェアラブル 端末	近年ではウェアラブル端末が様々な形で利用されるようになってきました。従業員の健康管理や、タスクのリマインドとしてスマートウォッチが利用されることもあります。これらの情報漏洩が、従業員の個人情報の漏洩に直結するリスクや、プライバシーの侵害、不正アクセスといったリスクが考えられます。
複合機	プリンターやスキャナーといった機能を提供する複合機は、ネットワーク接続やデータ保存機能により、サイバー攻撃や不正アクセスのリスクが高まります。未使用データの漏洩やプリントアウトされた機密情報の盗難、ソフトウェアの脆弱性からのマルウェア感染も懸念されます。

＊マルウェア（Malicious Software）：「悪意のあるソフトウェア」を略したもので、脆弱性や情報を利用して攻撃をするソフトウェアの総称

情報機器に有効なセキュリティ対策

☑ **暗号化**

紛失や盗難のリスクを回避するために、情報機器のデータを格納するハードディスクは暗号化するようにしましょう。OSが標準で暗号化機能を提供する場合もあります。

☑ **認証機能の強化**

暗号化したとしても、情報機器の不正利用を回避することはできません。情報機器によっては、指紋や顔といった生体認証機能が備わっているため、パスワードを組み合わせて強力な認証機能を提供するようにしましょう。

☑ **OSやファームウェア*の更新**

OSやファームウェアに潜むセキュリティホールを利用した攻撃が後を立ちません。常に最新の状態に更新することを徹底してください。

＊ファームウェア（Firmware）：機器内部に書き込まれ、その機器の動作や機能を担う「組み込みソフトウェア」のこと

☑ **セキュリティソフトの導入**

常に攻撃のリスクにさらされている情報機器を守るために、セキュリティソフトをインストールして、マルウェアなどの脅威から守るようにしましょう。

情報機器を利用するためのルールを明確にする

どんなに万全なセキュリティ対策をしていたとしても、情報機器を使う従業員がセキュリティ保護についての意識が醸成されていないと、セキュリティ事故はまぬがれないでしょう。杜撰な管理では紛失や漏洩は避けられませんし、不注意によって容易にマルウェアに感染してしまうかもしれません。場合によっては、悪意のある従業員による内部犯行が行われるかもしれません。

重要なことは、セキュリティポリシーに基づき、罰則を含めたセキュリティ規定を定め、これを従業員に周知して、ルールに基づく情報機器の利用を徹底することです。

第2節 会社·従業員のSNSをめぐる対策

企業におけるSNSの役割

企業にとってSNSの重要性が高まっています。フォロワーが情報を拡散してくれるSNSは、クチコミの効果が非常に高いと言えます。これは、フォロワーが自らのネットワークを通じて情報を広めることで、信頼性の高い情報が広く伝わり、商品やサービスの認知度が急速に向上するためです。

また、SNS上でのクチコミは、リアルタイムでの反応やフィードバックを得やすく、企業が消費者のニーズに迅速に対応することが可能となります。その結果、ブランドイメージや顧客満足度の向上に繋がります。

近年では、SNSが採用にも使われるようになりました。企業の社風や職場環境をアピールしやすく、安価で広範囲に情報発信できるため、採用とSNSは相性が良いと言えます。様々な場面で利用できるSNSは、その活用度合いが企業の競争力をも左右する存在となっているのです。

SNSが孕むリスク

SNS活用が拡大しているからこそ、SNSが孕むリスクにも注意を払う必要があります。一般的に、以下のようなリスクに注意する必要があります。

ブランドイメージの損失と炎上リスク	プライバシーの侵害や情報漏洩	アカウントの乗っ取り
SNS上での誤った情報発信や不適切な対応が、瞬時に拡散され、炎上する可能性があります。	SNSを通じた情報発信やサイバー攻撃により、機密情報や個人情報が流出する危険性があります。	パスワードが第三者に盗まれるとアカウントが乗っ取られ、意図しない情報発信等の恐れがあります。

SNSに対するセキュリティ対策

リスクを回避して安全なSNS運用を行うことで、SNSが持つメリットを最大限に活用することができます。SNSに対するセキュリティ対策として、以下のようなものが挙げられます。

SNS投稿のガイドラインを策定する

従業員がSNS投稿をする際に留意すべき事項や、注意点、ルールなどをまとめたガイドラインを作成します。その上で、SNS投稿に対する教育を実施します。

投稿前に承認プロセスを導入する

企業アカウントで誤解を招く表現や、不快感を与える表現が含まれると、瞬く間に炎上し、企業イメージが毀損します。投稿内容については、複数人でチェックするようにしてください。

パスワード管理を徹底する

類推されにくいパスワードにすることはもちろんのこと、たとえSNSの担当者であってもパスワードは秘密にしておくことが必要です。複数の端末から投稿する場合は、運用ルールを定めるとともに、パスワード以外の生体認証なども組み合わせると効果的です。

炎上した場合はどうする?

どんなに注意を払っても、SNSでは容易に炎上してしまうことが少なくありません。このような場合でも、冷静で誠実な対応が求められます。まずは、迅速に事実関係を行い、誤った情報や誤解があった場合は、正確な情報を公式に発信してください。

問題の原因を明らかにし、必要に応じて謝罪や改善策を提示すると良いでしょう。逆に、炎上した投稿を削除し、無かったことにしてはいけません。情報の拡散能力が高いSNSは、即座に削除しても、逆効果と考えてください。炎上には、誠実な態度で真正面から向き合うことが求められます。