企業を狙うサイバー犯罪
～今すぐできる会社のインターネットセキュリティ対策～

福岡県警察本部生活安全部サイバー犯罪対策課

1．はじめに

⑴狙われるのは中小企業

サイバー攻撃の標的は政府・自治体や重要インフラだけではありません。こうした大規模なサイバー攻撃には、数十台の端末から一斉攻撃をかける手口があり、それに使用される端末は攻撃者に乗っ取られた端末です。そして比較的セキュリティの甘い中小企業の端末が狙われています。最近では、大企業は防御が厳重なため、防御の甘い取引先の中小企業を狙い、そこから大企業のシステム内部へ侵入するケースも増えています。

⑵セキュリティ対策はなぜ必要なのか？

インターネットが社会生活の隅々まで普及している今、サイバー攻撃は社会機能や国民生活を脅かす大きな問題となっています。

個人も企業もセキュリティに関する正しい知識を身に付け、必要な対策を実践していくことがとても重要になっています。いったんサイバー攻撃を受けて被害を受けると、金銭の損失はもとより、顧客の喪失、業務の喪失など、経営に直結する重大なリスクが発生します。経営者が責任を問われたり、場合によっては株主代表訴訟の対象にもなります。

⑶すぐやろう！サイバーセキュリティ対策

セキュリティ対策は必要だと分かっていても直接利益を生み出すものではない、難しくてよく分からない、社内にITのことが分かる人材がいないなどの理由から、手つかずのままにしていませんか？最優先で実施すべき対策はそんなに難しいものではありません。基本的な対策を実施することで多くの攻撃を防ぐことができます。

2．中小企業における事例

地域・業種・従業員規模	事例
福岡県 卸売業 21～50名	（ウイルス被害事例）ウイルス対策ソフトの契約更新を失念し、数日間サポートが切れた。そのわずかの間に、インターネットに繋がっていたパソコンが「※1トロイの木馬」に感染した。 急きょアプリケーションを停止し、自社でリカバリーしたが、復旧までに約2か月を要し、その間、仕事にも支障を来した。
神奈川県 製造業 6～20名	（※2ランサムウェア被害事例）経営者宛てのメールに添付されているファイルを開いてしまった結果、「ファイルをロックしたので、解除してほしければ連絡をするように」と電話番号を含む警告画面がパソコンのスクリーン上に表示され消えなくなった。 社内の重要データは共有サーバで管理されており、バックアップ等を行っていたため会社としての被害はなかったが、個人の写真などのデータは参照できなくなっていた。
徳島県 農林水産業 6～20名	（経営にプラスの効果を発揮した事例）大手企業やコンプライアンス意識の高い農協等と取引を行う場合、社内の管理体制についての情報提供を求められることがある。 セキュリティ対策を含めた当社の管理体制は、取引先から評価され、安定した取引につながっている。

「中小企業における情報セキュリティ対策の実態調査-事例集-」情報処理推進機構（IPA）より抜粋編集

※1…正体を偽ってコンピューターへ侵入し、破壊活動を行うプログラム
※2…ランサム（身代金）のこと。メールに添付されたランサムウェアを不用意に開くと、パソコンのデータが勝手に暗号化されたり、パソコンがロックされたりして使用不可能となります。そして、暗号化ファイルの復元や、ロックの解除の引き換えに金銭を要求されます。

3．企業が受ける不利益

⑴金銭の損失

顧客の個人情報や取引先などから預った機密情報を万一漏えいした場合は、多大な損害賠償が発生します。また、インターネットバンキングの不正送金などで直接的な損失を被る企業も増えています。

⑵顧客の喪失

サイバー攻撃を受けた企業は管理責任を問われ、社会的評価は低下し、顧客離れなど大きなダメージを受けることになります。風評被害がいつまでも続き、イメージが回復せず事業の存続が困難になる場合もあります。

⑶業務の喪失

サイバー攻撃を受けると、被害の拡大を防止するため、システムを停止する措置が必要です。その間はメールすら使えなくなり、営業機会を喪失するとともに、社内の業務も停滞してしまいます。

⑷従業員への影響

内部不正が容易に行えるような職場環境は、従業員のモラルを低下させます。また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。

4．対策～情報セキュリティ５か条

⑴OSやソフトウェアは常に最新の状態にしよう！

OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。使用しているOSやソフトウェアに修正プログラムを適用する、若しくは最新版を利用しましょう。

⑵ウイルス対策ソフトを導入しよう！

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は常に最新の状態になるようにしましょう。

⑶パスワードを強化しよう！

パスワードが推測や解析されたり、ウェブサービスから窃取したID・パスワードが流用されることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。

⑷共有設定を見直そう！

データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため無関係な人に情報をのぞき見られるトラブルが増えています。クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。

⑸脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付きのメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

1．3～「中小企業向けサイバーセキュリティ対策の極意」（東京都産業労働局商工部調整課）より引用
4～　「情報セキュリティ５か条」情報処理推進機構（IPA）より引用

5．その他

福岡県内の中小事業者のサイバーセキュリティを支援するため、F-CSNET（福岡県中小事業者サイバーセキュリティ支援ネットワーク）を平成28年11月に発足しました。

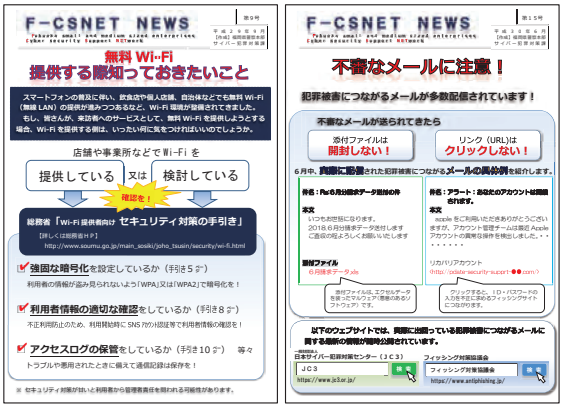
※構成機関団体

【公的機関】

九州経済産業局情報政策課、福岡県警察本部サイバー犯罪対策課、福岡県中小企業振興課

【中小事業者支援団体】

福岡県中小企業振興センター、福岡県商工会議所連合会、福岡県商工会連合会、福岡県中小企業団体中央会



【F-CSNET（エフシスネット） NEWS（ニュース）】

サイバー犯罪対策課では、中小事業者支援団体に発信しているF-CSNET NEWSをホームページ上で公開しておりますので、是非ご覧下さい。

福岡県警察ホームページ
www.police.fukuoka.jp/seian/seikei/h240401/security_2.html