リンクスグループ

SECURITY ACTION

独立行政法人情報処理推進機構（IPA）が実施する制度で
中小企業自らが、情報セキュリティ対策に取組むことを**自己宣言**する制度
安全・安心なIT社会を実現するために創設

★一つ星
中小企業の情報セキュリティ対策ガイドラインの「情報セキュリティ5か条」に取組むことを宣言した中小企業

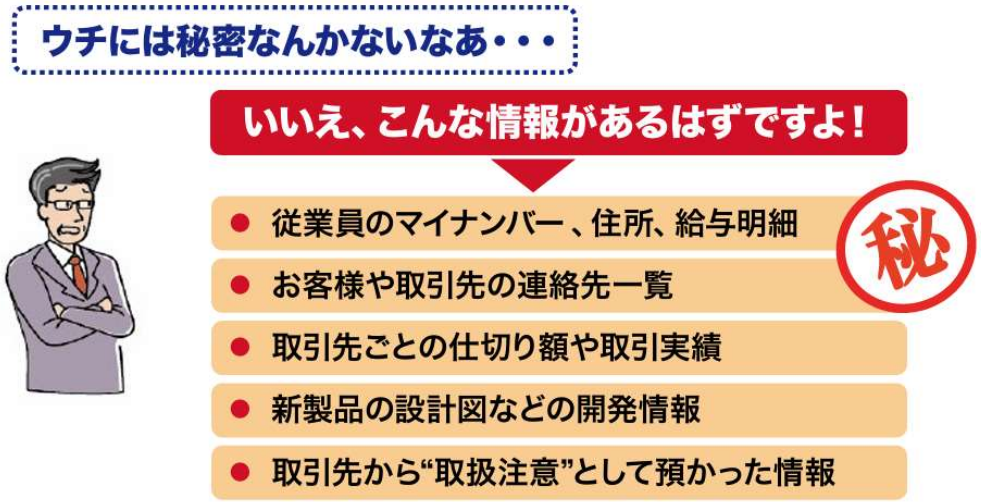
★★二つ星
情報セキュリティ基本方針を定め、外部に公開したことを宣言した中小企業

https://www.ipa.go.jp/security/security-action/

当社は『**一つ星**』に
取り組むと**宣言**しました

2024年7月29日

現状は・・・・



情報セキュリティですから、
個人情報に留まりません
会社にはいろんな情報があります。

会社情報全てについてセキュリティが出来ているでしょうか？
盗み出されませんか？

記録・記憶媒体別に情報セキュリティーが出来ているでしょうか？
今回は、次項上げる
５か条に取り組んで行くという「宣言」になります。

情報セキュリティ対策状況等を、誰かが認定するものではありません。
また、出来なかったからと言って、罰則は有りません。

リンクスグループ

何に取り組むか

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！

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、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。お使いの OS やソフトウェアには、修正プログラムを適用する、または最新版を利用するようにしましょう。

対策例
- WindowsUpdate、(WindowsOSの場合)、ソフトウェア・アップデート(macOSの場合)などベンダの提供するサービスを実行する。
- Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする。
- テレワークで利用するパソコン等のソフトウェアやルーター等のファームウェアを最新版にする。
- 利用中のソフトウェアに脆弱性が存在しないか、MyJVN バージョンチェッカ※で確認する。

※パソコンにインストールされているソフトウェア製品が最新かどうかを簡単な操作で確認できるツール　https://jvndb.jvn.jp/apis/myjvn/

2 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。

対策例
- ウイルス定義ファイルが自動更新されるように設定する。
- 統合型のセキュリティ対策ソフトの導入を検討する。
- OSに標準搭載されているセキュリティ機能を有効活用する。
- テレワークで利用するパソコン等の端末にウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にする。

3 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流出した ID・パスワードが悪用されたりすることで、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。

対策例
- パスワードは10文字以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。
- 同じID・パスワードを複数サービス間で使い回さない。
- テレワークでVPNやクラウドサービスを利用する際は、強固なパスワードを設定し、可能な場合は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！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

対策例
- 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。
- 従業員の異動や退職時には速やかに設定を変更(削除)する。
- テレワークで使用するパソコン等は他者と共有しない。共有せざるを得ない場合は、別途ユーザーアカウントを作成する。
- 外出先でフリーWi-Fiを使うときにはパソコンのファイル共有をオフにする。

5 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。

対策例
- IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る。
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する。
- テレワークでは管理者が従業員に適宜注意喚起し、従業員はセキュリティの懸念は速やかに報告する。

当社の現状を見てみますと

←ソフトは**自動で更新。**

←ウイルス対策ソフトは導入済み
自動更新

←パスワードは意識してるが・・・
PW知識の復習や利便性と危険性を再認識

←共有設定は現在システムがない
ファイルサーバ、ネットプリンター等が入ったら検討

←手口は時々刻々と変わっています
最新情報を随時伝達して行く

ほぼ出来上がっており、少しレベルアップしてから「★★二つ星」の申請が可能です

リンクスグループ

どう進めるか

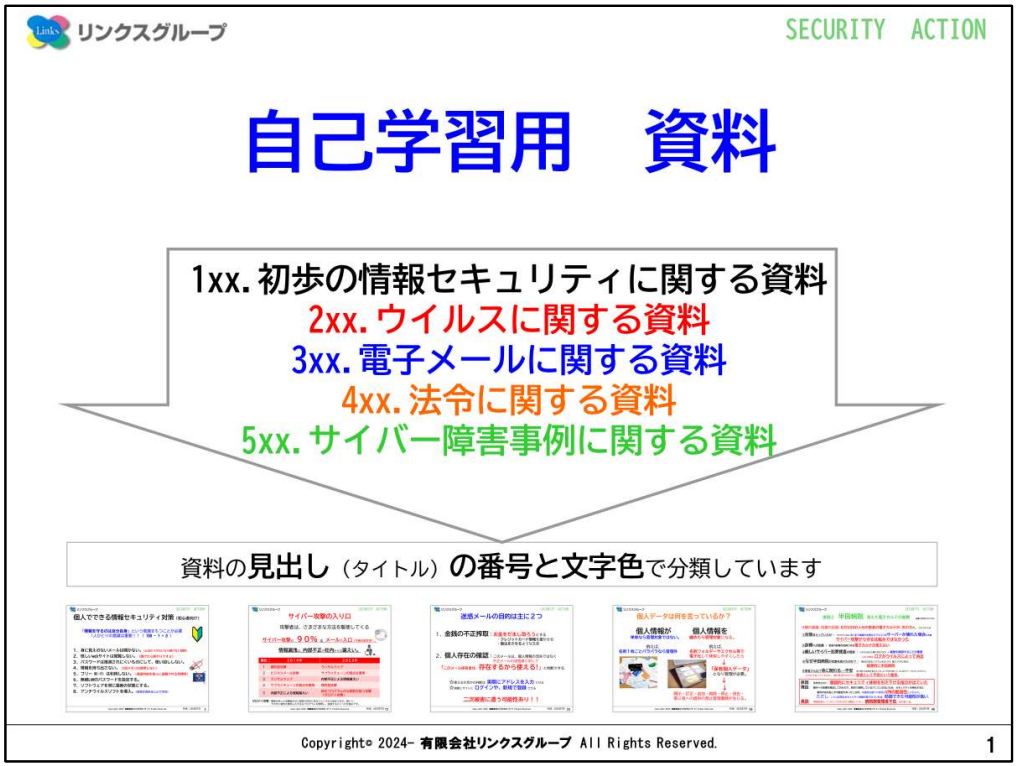
登録マークは、ＨＰ、会社案内、名刺等に掲載します。

当社は、全員が一同に揃う事は稀なので、集合教育ではなく
月に１～2回、学習用の情報を流して自己学習していただく。
疑問や質問が有れば、メールや電話等で問い合わせる。

学習資料の初期は
５テーマで用意し
一件A4サイズ一枚を基本とする

既に、netや一般ニュースで
既知情報かもしれませんが
復習として読んでください。
社会の動きも捉えて行きます。

この資料を積算すれば、当社のセキュリティ学習資料になります。



担当：maruoka