中小企業ユーザーの主な声

●自社の対策が不十分であることにより、**取引先に迷惑をおかけするわけにはいかない**ため、サイバーセキュリティお助け隊サービスの導入を決めた。

●検知・監視してくれるだけでなく**何かあった時の事後対応まで含まれる**ところがよい。セキュリティについて全く分からないので、**まとめてお任せできるところにお願いしたい**と考えていた。

●アラート通知が来るので、**防御できていることが実感でき安心**。本社のほか複数の拠点でも利用しているが**サービス利用料が安いので助かって**いる。

●**何も無いということがわかる**ことも良い点。**セキュリティレポートをストックしておくことで、報告資料としても使える**ので助かっている。

※サイバーセキュリティお助け隊サービス提供事業者　提供情報より

PRサイトのご紹介

- サイバーセキュリティお助け隊サービスのPRサイトを公開中。分かりやすく親しみやすい動画コンテンツとともに登録サービスを紹介。

https://www.ipa.go.jp/security/otasuketai-pr/

経済産業省 商務情報政策局
サイバーセキュリティ課長
武尾 伸隆 様の推奨コメントを
掲載しております。

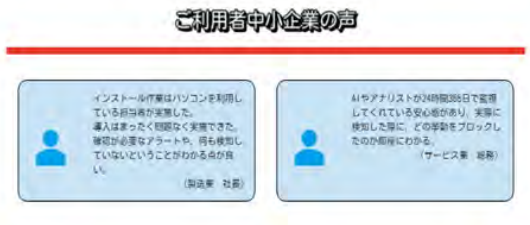
推奨コメント

2分40秒のサイバー
セキュリティお助け隊
サービスのプロモー
ション動画。

動画コンテンツ

掲載内容

ご利用者
中小企業の声



お助け隊サービスを
利用されている中小
企業様の声を掲載
しています。
（今後追加予定）

IT導入補助金に関する
お知らせ

IT導入補助金のお助け隊
サービスとの連携についての
説明と、申請方法について
お知らせしております。

参考情報

- 中小企業向け普及促進ツールのご紹介

  普及促進ツール（チラシ・パンフ）を
  是非ご活用ください

  IPAのWebサイトからもダウンロードできます。

  https://www.ipa.go.jp/security/sme/list.html

SECURITY ACTION 制度解説

SECURITY ACTION 制度概要

- 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
  - 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに2段階の取組み目標を用意

1段階目（一つ星）

「情報セキュリティ5か条」に取組むことを宣言

2段階目（二つ星）

「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、「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

  - SECURITY ACTION 自己宣言数35万件を突破！（2024年6月）

SECURITY ACTION 制度の特長

- 情報セキュリティ対策への取組みの見える化
  - ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに印刷することで自らの取組み姿勢をアピール
- 顧客や取引先との信頼関係の構築
  - 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに
- 公的補助・民間の支援を受けやすく
  - SECURITY ACTIONを要件とする補助金の申請、普及賛同企業等から提供される様々な支援策が利用可能

普及賛同企業等

SECURITY ACTION 制度の趣旨に賛同し、当制度の普及促進のための積極的な取組みを実施する企業及び団体等。中小企業等が SECURITY ACTION制度を活用し、情報セキュリティ対策に取組むことを自己宣言するための支援策等を提供

【普及賛同企業等が提供する支援策の例】

- セキュリティに関する情報提供
- セキュリティ体制の構築を支援
- セキュリティ関連サービス提供時に優遇

登録事業者数　464社（2024/6時点）

SECURITY ACTION公式サイト

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

- SECURITY ACTIONの制度紹介や申込(宣言)、セキュリティ対策推進に役立つ情報・ツールを提供

ロゴマークの
使用申込(宣言)

SECURITY ACTION 公式 **検索**

ロゴマーク申込手順

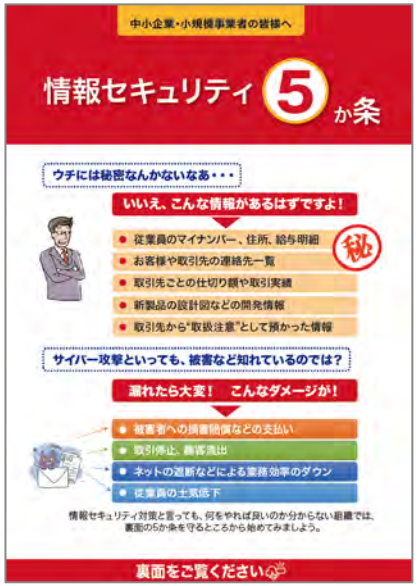

STEP 1
取組目標を決める
STEP 2
申込みフォームに入力
STEP 3
申込み手続き完了
STEP 4
ダウンロード
SECURITY ACTION ★
SECURITY ACTION ★★
一つ星 or 二つ星のどちらを宣言するか、取組目標を決めてください。
ロゴマーク使用規約に同意後、自己宣言のお申し込みを行います。
STEP2 の後、1 週間程度で自己宣言 ID をお知らせするメールが届きます。
STEP3 の後、1～2週間程度でロゴマークのダウンロード方法をお知らせするメールが届きます。
SECURITY ACTION公式サイト
https://www.ipa.go.jp/security/security-action/

一つ星

一つ星の取組み目標

- 「情報セキュリティ5か条」に取組むことを宣言

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



1. OSやソフトウェアは常に最新の状態に

- 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る
- 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、もしくは最新版を利用する

＜対策例＞

- Windows Update(Windows OSの場合)/
  ソフトウェア・アップデート(Mac OSの場合)/
  OSバージョンアップ(Android の場合)
- Adobe Reader/Java実行環境(JRE) など
  利用中のソフトウェアを最新版にする

2. ウイルス対策ソフトを導入

- 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る
- 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する

＜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(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)を導入する

3. パスワードを強化

- 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る
- パスワードは「長く」「複雑に」「使い回さない」ようにして強化する

＜対策例＞

- パスワードは英数字記号含めて長い文字数にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 同じID・パスワードをいろいろなウェブサービスで使い回さない

4. 共有設定を見直す

- 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る
- 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する

＜対策例＞

- ウェブサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、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設定の変更(削除)漏れがないように注意する

5. 脅威や攻撃の手口を知る

- 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る
- 脅威や攻撃の手口を知って対策をとる

＜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

二つ星

二つ星の取組み目標

- 「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、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

＋

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

1. 基本方針の作成と周知

- 経営者が定めた情報セキュリティに関する基本方針を、従業員や関係者に伝えるために簡潔な文書を作成・周知する
- 中小企業の情報セキュリティ対策ガイドライン付録「情報セキュリティ基本方針（サンプル）」を参考

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

2. 実施状況の把握

- 自社のセキュリティ対策の実施状況を把握するために「5分でできる!情報セキュリティ自社診断」を活用する
  - 25項目の設問に答えるだけで、自社の情報セキュリティの問題点を簡単に把握できる
  - 解説編の対策例を参考に、社内ルールを作成することができる
  - 付録の情報セキュリティハンドブックを活用すると従業員に対する社内ルールの周知が簡単にできる

基本的対策

- 情報セキュリティ自社診断の「基本的対策」は、情報セキュリティ5か条を質問化したもの

No.	診断内容	実施している	一部実施している	実施していない	わからない
1	パソコンやスマホなど情報機器のOS やソフトウェアは常に最新の状態にしていますか？	4	2	0	-1
2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	-1
3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	-1
4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	-1
5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	-1

※1　コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる
※2　営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のこと

5分でできる!情報セキュリティ自社診断

従業員としての対策

No.	診断内容	実施している	一部実施している	実施していない	わからない
6	電子メールの添付ファイルや本文中のURL リンクを介したウイルス感染に気をつけていますか？	4	2	0	-1
7	電子メールやFAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	-1
8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	-1
9	無線LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	-1
10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	-1
11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	-1

5分でできる!情報セキュリティ自社診断

従業員としての対策

No.	診断内容	実施している	一部実施している	実施していない	わからない
12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	-1
13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	-1
14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	-1
15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	-1
16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	-1
17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	-1
18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	-1

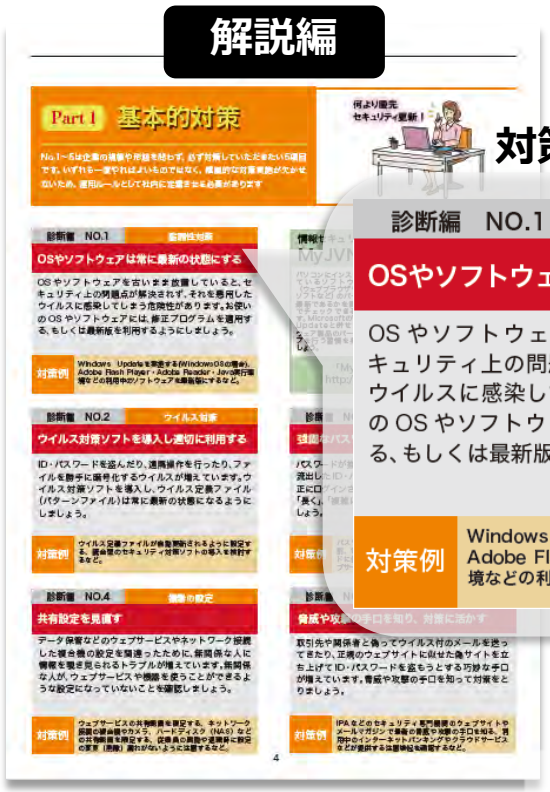
5分でできる!情報セキュリティ自社診断

組織としての対策

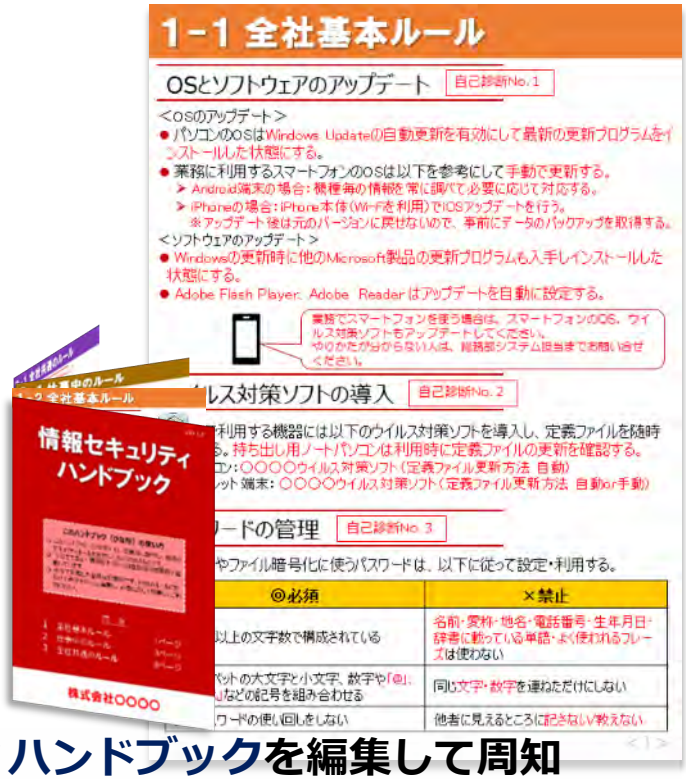
No.	診断内容	実施している	一部実施している	実施していない	わからない
19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	-1
20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	-1
21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	-1
22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	-1
23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	-1
24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	-1
25	情報セキュリティ対策(上記1 ～ 24 など)をルール化し、従業員に明示していますか？	4	2	0	-1

3. 対策の決定と周知

- 問題があった項目は、解説編を参考に対策を決定
- 付録「情報セキュリティハンドブック(ひな形)」を編集して社内周知する



対策例を参考にして決定



情報セキュリティハンドブックを編集して周知

参考資料

● 中小企業の情報セキュリティ対策ガイドライン

中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン

https://www.ipa.go.jp/security/guide/sme/about.html

● SECURITY ACTION

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

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