損害保険・生命保険総合代理店

アイ・エス・アイからのお知らせ

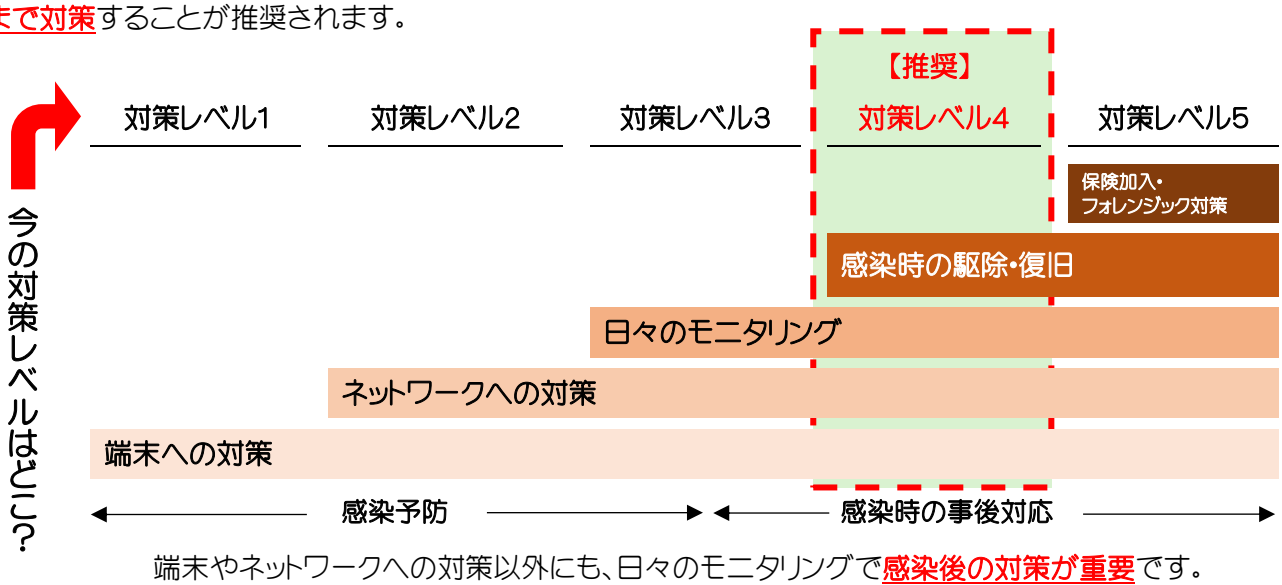
取り返しのつかないことになる前に

「対策レベル」を確認してください！

いつも大変お世話になっております。最近新聞やニュースでも多く目にするようになってきたサイバー攻撃。
企業規模の大小に関わらず、自然災害のようにいつ誰もが被害にあってもおかしくない状況になってきました！
そこで緊急情報提供として、現状のセキュリティ対策確認とアップデートの資料をお作りしましたのでご覧ください！

■ 要確認！中小企業が対応すべき基準

手口が巧妙化・複雑化するサイバー攻撃はすべてを防ぐことは困難なため、近年では事故が起きたとしてもその被害を最小限に食い止めるような対応が重要視されており、「対応すべき基準」としては、少なくとも下記レベル 4 まで対策することが推奨されます。



端末やネットワークへの対策以外にも、日々のモニタリングで感染後の対策が重要です。

（出展）内閣サイバーセキュリティセンター　中小企業のセキュリティ対策とクラウド活用

■ どうする！どうなる！？ウイルスセキュリティを通過したとき…

「初犯（未知・新種）」のウイルスがウイルス対策ソフトをすり抜けてきてしまう！

日々のモニタリングができていないと…

企業がサイバー攻撃に気付くまで平均207日！　発覚の約9割が第三者からの指摘

※IBM 「Cost of a Data Breach Report 2022」

今すぐできるアクションプランと具体的な対策方法は裏面に！

■ まずは社内で今すぐやってほしいこと

IPA提供の「情報セキュリティ5か条を守る！」を全員に周知！
IPA提供の「5分でできる！情報セキュリティ自社診断」を実践！

IPA 自社診断

■ 担当者を決めて取り組んでほしいこと

(1) 管理体制の構築
　①責任分担と連絡体制の整備
　②緊急時対応体制の整備
(2) デジタルトランスフォーメーション(DX)の推進と情報セキュリティの予算化
(3) 情報セキュリティ規程の作成
　①対応すべきリスクの特定
　②対策の決定
　③規程の作成
　　IPA提供の「情報セキュリティ関連規程(サンプル)」を活用！
(4) 情報セキュリティ委託時の対策
(5) 点検と改善
　資料①②に基づく点検

(参考) IPA 独立行政法人　情報処理推進機構
中小企業の情報セキュリティ対策ガイドライン第 3.1 版

■ セキュリティ通過！万一の感染対策を具体的に考える！

✔対策レベル1～3 【事前対策　侵入・感染の予防】
　・セキュリティ担当者を置く、社内規定を作成する
　・UTM(総合脅威管理、ファイアウォール、アンチウイルス)を検討、導入する
　・NGAV(次世代型アンチウイルスソフトなど)を検討、導入する

✔対策レベル4～5 【事後準備　侵入・感染後の対処】
　・事象発生時の対応事前確認(誰がどうするのか？)

検知・初動対応 → 報告・公表 → 復旧・再発防止

　・EDRの導入(常時監視し、異常や不審な挙動が発生した場合に通知、復旧する)
　・サイバー保険を検討、導入する(お任せください！)
　　第三者に対する賠償費用、事故発生時の各種対応費用、逸失利益・営業継続費用の準備
　　損害保険会社提供のサポートデスクを知っておくのも有効な手段ではないでしょうか？

最後までご覧いただきありがとうございます。御社のセキュリティ対策はいかがでしたでしょうか？
会社の大切な資産を守るため、今後も有益な情報がありましたら引き続きご提供したいと思います。

ひとつでもご心配なところがありましたら、お気軽にご連絡・ご相談ください

弊社のネットワークを生かし、IT―BCP(事業継続計画)をお手伝いします！

お問合せは・・・　有限会社アイ・エス・アイ　/　函館市駒場町 5-26　/　TEL 0138-53-5539