

サイバー攻撃者の目的



「当社には狙われるような情報はない」
いいえ、攻撃者は情報の価値は問いません！

サイバー攻撃で起きる被害

情報漏洩

個人情報／知的財産
企業秘密／賠償金

業務の停止

機会損失／
人命への危険（医療現場）
サービス停止／復旧費

被害者から加害者へ

踏み台による
他社への攻撃

あなたの会社を起点に、取引先企業先のさらに先
サプライチェーン全体に影響を及ぼすことに・・・

情報漏洩賠償額は高額化

顧客情報漏洩

2007年 東京地裁

アンケートデータや資料請求のために入力されたデータなど
5万人分のデータが外部から閲覧できる状態になっており、
迷惑メールが送られてくる等の二次被害も確認された。

1人あたり

賠償判決 **35,000円**

2016年 個人情報漏洩事故

件数	468件
漏洩人数	1396万人

1人あたり

想定平均損害賠償額 **31,646円**

※JNSA 2016年情報セキュリティインシデントに関する調査報告書

元気の Best Advice



経営者様、企業様の中でサイバー攻撃に対する危機意識を持たれている割合は増えています。ただ、「どのような対策をすれば良いのかわからない。」そういった声が多いというのが現状です。

今までサイバー攻撃の事例に直に携わってきたのは、被害を受けた企業や公的機関、一部の専門家や保険会社のみに限られていました。いわば得体の知らないリスクがサイバー攻撃のリスクです。サイバー攻撃のリスクはインターネットの普及やITの発達とともに生まれたリスクであり、ほとんどの方にとっては経験の無い未知のリスクです。

私たちは、未来を目指す企業にとって避けては通れないリスクであると確信しており、今後益々力を入れて普及を目指す商品と位置付けています。当社では今春IT企業出身者を採用し、サイバー攻撃についての研究、保険提案に重点を置いています。

皆様の挑戦を支えていくため、私たちも新しい挑戦を続けています。
今一度、サイバーリスクという新しい脅威に備える準備を進めましょう。

賠償シリーズ②



「社長！」

社内の情報が漏れているようです。

どうすればいいですか？」

被害拡大防止の
指示をすぐに出せますか？

「コピー機から火が出ている。」
こんな報告には消火器で火を消すよう直ちに指示を出すと思います。

企業は、被害拡大を防ぐ指示が出せる火災リスクにはすでに、保険で備えています。

被害拡大防止の指示ができないリスク、
どのくらいの被害が出るかわからないリスク、
だからこそ保険で備えるべきと私たちは考えます。



サイバー攻撃はすぐそこまできている

情報漏洩は他人ごとではない