2024 年 3 月 12 日

株式会社瀧神巧業　代表取締役　佐藤慎

サイバーセキュリティ体制について

1、サイバーセキュリティ体制策定の目的

総務省「サイバー攻撃に関する最近の動向-令和 3 年 6 月 29 日-」によると不正アクセスは 2018 年～2019 年で 2 倍の増加、フィッシングの報告件数は 2020 年 2 月～2021 年 1 月の間で約 35,000 件も増えている。大手企業がサイバー攻撃を受け、機密情報や個人情報が流出しています。情報漏洩を防ぐため、当社でもサイバーセキュリティ体制を定める。

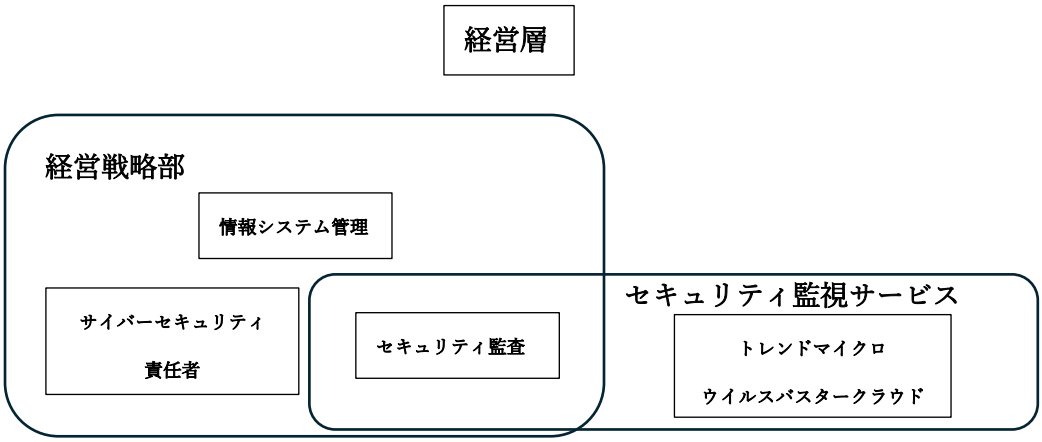
2、サイバーセキュリティ体制について

個人情報保護法に従い、「個人情報」氏名、生年月日、住所、顔写真などで特定の個人を識別できる情報を個人データとし違法な行為を助長させず安全管理を徹底し個人データの漏えいを防止する。

3、サイバーセキュリティ責任者・体制図

サイバーセキュリティ責任者：佐藤敦也

体制図



4、サイバーセキュリティ対策

⑴リスクアセスメント表作成

① 年 1 回実施

② 作成後責任者が社長に提出する

⑵サイバーセキュリティリスク管理に関する KPI の指標

① 対策を行わなかった時の被害額

② セキュリティ研修の受講率

③ サイバーセキュリティー対策に従事する要因のスキルの自己評価

④ 組織におけるセキュリティ成熟度の評価

⑶KPI に応じた PDCA サイクル

① 毎月末日実施する

② 振り返りを社長・部署長へ提出する

5、重大インシデント発生時についてと注意すべきこと

⑴インシデントの発生が懸念される場合に、経営者ほか関係者に速やかな報告を行う。

⑵サイバー攻撃を受けた端末の確保と情報の保全を行う。

⑶感染内容の調査と流出データの確認を行い 2 次被害を防ぐ

⑷弁護士へ相談し適切な対応を検討する

⑸情報漏洩発覚から 3 日～5 日以内に、個人情報保護委員会へ「速報」を提出する

⑹30 日以内に「確報」を提出する

⑺被害者への報告と謝罪を行う

⑻漏洩した社員が不法行為責任を負い、相手に生じた損害を賠償する

注)

⑼個人情報保護委員会からの処分を受ける可能性がある

⑽国からの是正勧告に従わなかった場合、最大で 6 ヶ月の懲役または最大 30 万円の罰金

⑾不正な利益を得る目的で漏洩した場合、罰則はより重くなり、1 年以下の懲役または 50 万円以下の罰金

⑿会社にも 50 万円以下の罰金が科される場合がある