

2026年1月1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。

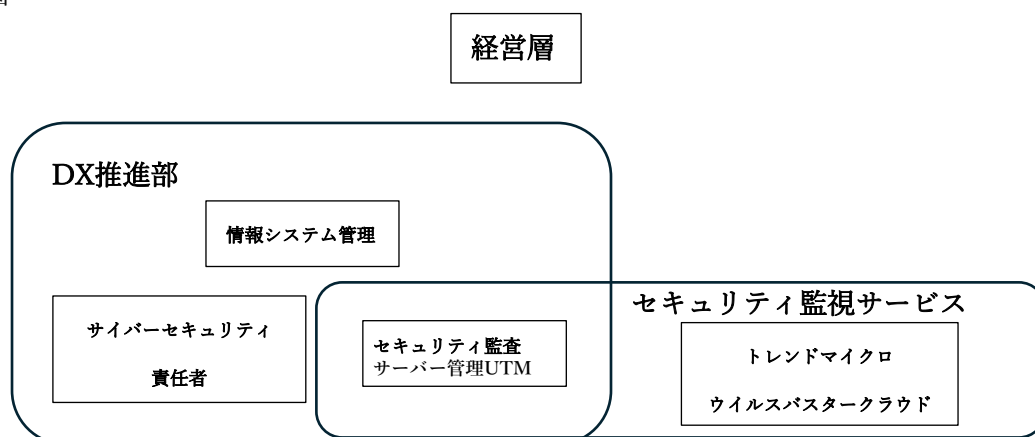
2、サイバーセキュリティ体制について

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

(1) 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

(2) 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

(3) KPI 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

- (1)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。
- (2)サイバー攻撃を受けた端末の確保と情報の保全を行う。
- (3)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
- (4)弁護士へ相談し適切な対応を検討する
- (5)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
- (6)30日以内に「確報」を提出する
- (7)被害者への報告と謝罪を行う
- (8)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)
- (9)個人情報保護委員会からの処分を受ける可能性がある
- (10)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
- (11)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
- (12)会社にも50万円以下の罰金が科される場合がある