UHY Tokyo & Co
Certified Public Accountants

総務省：「サイバーセキュリティ対策情報開示の手引き」を公表

UHY Tokyo ニュースレター / 2019年9月

総務省は2019年6月28日、「サイバーセキュリティ対策情報開示の手引き」を公表しました。

本手引きでは、サイバーセキュリティ対策に対する社会的要請は非常に大きくなっており、企業における重要な経営課題の一つとして位置づけられるべきものとなっているとし、企業として社会的責任を果たし、ステークホルダーからの信頼を得るためには、サイバーセキュリティ対策に係る適切な情報開示が重要であるとしています。

一方でサイバーセキュリティ対策の詳細を開示した場合には逆にサイバー攻撃等を誘発するリスクもあることから、本手引きでは開示項目の例を示すとともに、既に公開されている開示書類の事例集を掲載することで、各企業が情報開示の在り方を検討する際の参考資料となることを目的としています。

主な内容は下記の通りであり、本手引きの全文は下記URLからご確認ください。

http://www.soumu.go.jp/main_content/000630516.pdf

１．情報開示手段

情報開示に活用されている開示書類として以下挙げられており、対策の記載量は任意開示の方が比較的に多い傾向にあると記載されています。

- 有価証券報告書（制度開示）
- コーポレート・ガバナンス報告書（制度開示）
- CSR報告書／サステナビリティ報告書（任意開示）
- 統合報告書（任意開示）
- アニュアルレポート（任意開示）
- 情報セキュリティ報告書（任意開示）

２．開示にあたってのポイント

開示にあたって留意すべき点として以下挙げられており、ステークホルダーに対して有益と思われる情報を提供する必要があると記載されています。

- 目的適合性
- 表現真正性
- 比較可能性
- 理解容易性
- 適時公表性

本手引きでは、情報セキュリティ対策に係る情報開示の在り方や開示するポイントが整理されており、各企業において情報を開示する上での参考資料として活用されることが期待されています。

ご質問やご要望がございましたらお気軽にお問い合わせください。

※なお、本稿の意見に関する部分は、筆者の個人的な見解であることをあらかじめお断りします。

コンタクト

UHY東京監査法人
小野 琢司 – IT・内部統制 PG
Email: takuji.ono@uhy-tokyo.or.jp

〒107-0052 東京都港区赤坂 7-3-37 プラース・カナダ 3F
Tel: +81 3 5410 1391 / Fax: +81 3 5410 2474
Website : http://www.uhy-tokyo.or.jp/