資料８－１

「サイバーセキュリティ対策情報開示の手引き（仮称）」骨子案

Ⅰ．サイバーセキュリティ対策情報開示の手引き（仮称）

１．本手引き（仮称）の趣旨・目的

※　サイバーセキュリティ対策の情報開示の意義、手引きの目的、活用主体、対象とする情報開示など、本手引き（仮称）の前提について記載。

※　サイバーセキュリティリスクの増大と対策の重要性について触れる。

※　なお、サイバーセキュリティの定義はサイバーセキュリティ基本法における「サイバーセキュリティ」を引用。

※　対策としては、主にサイバーセキュリティ経営ガイドライン等を参照。一方で、手引きの活用主体としては、経営者ではなく、主に企業における開示書類の作成の実務的な担当者を想定。

２．情報開示の手段

※　例えば以下のような典型的な開示書類について、文書としての概要を紹介する。

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

３．企業における情報開示の在り方

…サイバーセキュリティ経営ガイドライン等から抽出した対策の開示

①サイバーセキュリティ対応方針策定
②リスク管理体制の構築
③資源（予算、人員等）の確保
④リスクの把握と対応計画策定
⑤保護対策（防御・検知・分析）の実施
⑥ＰＤＣＡの実施
⑦緊急対応体制の整備
⑧復旧体制の整備
⑨サプライチェーンセキュリティ対策
⑩情報共有活動への参加
⑪グループ単位のサイバーセキュリティ対策

※　企業におけるサイバーセキュリティ対策としては、いずれも重要であり、利用者等からすれば、これらの実施状況が開示されることにより、商品・サービスの選択など

の際の参考になると考えられる。一方で、例えば、サイバー攻撃への対応計画（④）や保護対策（⑤）を具体的に開示した場合は、サイバー攻撃等を誘発するリスクもあることから、④、⑤、⑦、⑧、⑨、⑪などについては開示する内容に留意が必要。

※　具体的な事例を踏まえた記載例（抽出）を掲載。

※　開示書類に対する第三者意見、サイバーセキュリティ対策の認証取得等、情報開示の信頼性を高めるための補足的手段を記載することが望ましい。手引きにおいては、具体的な事例を踏まえた記載例（抽出）を掲載。

４．手引き（仮称）のメンテナンスのプロセスについて

※　本手引きについて、企業における開示状況やサイバーセキュリティの動向を踏まえ、関係者の意見も踏まえつつ、適宜見直しの検討を行う。

５．関連ガイドライン等の紹介

※　例えば、「サイバーセキュリティ経営ガイドライン」や「企業経営のためのサイバーセキュリティの考え方」、ICT ガバナンスの向上に役立つ施策のリンク等、本手引きの内容・背景の理解の深化や開示の取組に有用と考えられるものを紹介。

Ⅱ．サイバーセキュリティ対策の情報開示に係る事例集

【東証一部上場企業における事例】

…Ⅰの各項で記載した内容が含まれた実際の開示書類を事例集として添付

※　任意開示の書類（CSR 報告書／サステナビリティ報告書、情報セキュリティ報告書、統合報告書、アニュアルレポート等）から具体的な事例を選定。

※　個別の表現等に必要な注釈やコメントを付す。

※　企業名を公表するかどうかについて要検討（例えば、業界だけ明示して企業名をマスキングする等も視野に入れる）。

※　「３．」の各項目との対応関係をわかりやすく明示することを想定。