

「セキュリティ対策情報開示の手引き（仮称）」骨子案

I. 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

- ※ 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

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
 - ・情報セキュリティポリシー
 - ・情報セキュリティ基本方針等

3. 企業における開示のレベルに応じた情報開示の在り方

3 - 1. セキュリティ対策が非開示または限定的である事業者

…主要 5 項目の開示

- ①セキュリティに関する基本方針等の策定状況
- ②セキュリティに関する管理体制
- ③社員に対する教育・人材育成
- ④社外との情報共有体制
- ⑤第三者評価・認証の取得状況

- ※ 具体的な事例を踏まえた記載例（抽出）を掲載。
- ※ 媒体ごとの記載ではなく、あくまで項目の紹介を行う。

3 - 2. 既に情報開示に取り組んでいる事業者

…「情報セキュリティ報告書」から抽出した記載項目の開示

- ①基礎情報
- ②経営者の情報セキュリティに関する考え方（特に情報セキュリティに関する取組方針、対象範囲）
- ③情報セキュリティガバナンス（特に情報セキュリティマネジメント体制（責任の所在、組織体制、コンプライアンス等）
- ④情報セキュリティ対策の計画、目標
- ⑤情報セキュリティ対策の実績、評価（実績）
- ⑥情報セキュリティに係る主要注カテーマ

⑦（取得している場合の）第三者評価・認証等

- ※ 具体的な事例を踏まえた記載例（抽出）を掲載。
- ※ 「情報セキュリティ報告書モデル」そのものの作成ではなく、あくまで項目の紹介を行う。

…セキュリティインシデントやそれを受けた対策等に係る情報開示

- ※ 具体的な事例を踏まえた記載例（抽出）を掲載。

…グループ全体・サプライチェーン全体のセキュリティ対策の情報開示

- ※ 具体的な事例を踏まえた記載例（抽出）を掲載。

4. 情報開示の信頼性を高めるための補足的手段について

- ※ 開示書類に対する第三者意見、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紹介
- ※ 具体的な事例を踏まえた記載例（抽出）を掲載。

5. 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、年度単位を基本としつつ、必要に応じて関係者の意見を踏まえながら見直しの検討を行う。

6. 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. 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）。