

- 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。

企業（群）

企業がとるべき対策（※）

ステークホルダー

経営層

従業員

グループ会社

外部委託・調達先

- 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
- ⑥P D C A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グループ単位のセキュリティ対策



ウォッチ

取引先

情報共有団体/コミュニティ

投資家、株主
アナリスト

市民
一般消費者

悪意の攻撃者

（※）サイバーセキュリティ経営ガイドライン等を参照