サイバーセキュリティ基本方針

SBI VC トレード株式会社（以下、「当社」といいます。）は、サイバー攻撃に対するセキュリティ対策を重要な経営課題であると認識し、サイバーセキュリティ基本法、サイバーセキュリティ経営ガイドライン、その他サイバーセキュリティに関する関係諸法令等を遵守するとともに、サイバーセキュリティ管理態勢を継続的に整備・改善します。

1. 目的・方向性

当社は、サイバーセキュリティ対策の目的と方向性を明確にし、当社の経営目標の達成およびお客様・地域社会・株主・当局等の関係主体からの要求事項、ならびに法規制等への適切な対応を行います。

2. ガバナンス（取締役会等・経営陣のコミットメント）
    1. 取締役会等は、サイバーセキュリティリスクを組織全体のリスク管理の一部として捉え、本基本方針を策定します。
    2. 経営陣は、サイバーセキュリティリスクを認識のうえ、自らリーダーシップを発揮し、対策を推進します。
    3. 経営陣は、定期的にサイバーセキュリティ管理態勢のレビューを実施し、十分な検証・議論を行います（必要に応じ外部専門家レビューを含む）。
    4. 経営陣は、基本方針に基づき、戦略および取組計画（複数年計画を含む）を策定し、年次および重要な変更時に見直します。

3. 管理態勢の構築（CISO、SOC/CSIRT、報告体制）
    1. 経営陣は、サイバーセキュリティを統括管理する責任者（CISO 等）を任命し、役割・責任・権限を明確化します。
    2. 当社は、早期警戒のための情報収集・共有・分析体制、SOC 等の監視体制（外部活用を含む）、CSIRT 等の緊急時対応体制（報告・広報体制を含む）を整備します。
    3. 当社は、サードパーティ由来のリスクを含め、組織横断の報告・連絡・協議ルートおよび指揮命令系統を整備します。
    4. 経営陣は、定期的にリスク状況・リスク評価結果・取組計画の進捗等の報告を担当部署等に求めます。

4. 規程・業務プロセスの整備

当社は、サイバーセキュリティに係る規程および業務プロセスを整備し、定期的に見直します。規程等には、情報資産管理、リスク評価、脆弱性管理、脆弱性診断/侵入テスト、演習・訓練、認証・アクセス管理、教育・研修、データ管理、ログ管理、セキュリティ・バイ・デザイン、技術的対策、インシデント対応・復旧、サードパーティリスク管理等を含め

ます。

5. 経営資源の確保・人材育成

経営陣は、専門性を有する人材の配置および必要な予算配分を行い、基本方針と整合的な人材育成・確保の計画（育成/採用/教育研修・訓練計画等）を策定します。また、経営陣自らも研修・訓練等に参加し、ガバナンスと組織風土の醸成に努めます。

6. 技術的対策と検知・対応能力の向上

当社は、情報システムのセキュリティ対策として適切な情報機器を導入し、サイバー攻撃に対する検知・対応能力の向上に努めます。

7. 外部委託先を含む総合的な対策

当社は、外部業務委託先を含めた総合的なセキュリティ対策の整備に努め、サードパーティリスクを踏まえた管理を行います。

8. 牽制・内部監査（3 線防衛）

内部監査部門は、独立した立場からリスクベース・アプローチに基づく内部監査を実施し、重要事項を遅滞なく代表取締役および取締役会等に報告し、改善状況を把握します。

9. 情報連携・情報開示

当社は、サイバーセキュリティリスクや対策にかかる情報連携・情報開示に努めます（攻撃者の攻撃を助長する可能性に配慮しつつ、適切に実施します）。

2026 年 3 月 11 日

SBI VC トレード株式会社
代表取締役社長 近藤 智彦