情報セキュリティ基本方針

株式会社 QueeenB（以下、当社）は、ラボオートメーションシステムの開発・提供を行う企業として、お客様や研究機関からお預かりした研究データや機密情報、並びに当社が保有する技術情報などの情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1. 経営者の責任

- 当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。
- 経営者は事業戦略との整合性を図りながら、十分なリソースを確保し、情報セキュリティが企業価値向上の基盤となるよう指揮・監督を行います。

2. 社内体制の整備

- 当社は、情報セキュリティを維持および改善するために責任者および担当部門を設置し、必要な規程や手続きを社内の正式な規則として定めます。
- ラボオートメーションや AI システムなど、当社が提供するサービスや製品に対しても明確なセキュリティ基準を策定し、運用します。

3. 従業員の取り組み

- 当社の従業員は、情報セキュリティに関する知識・技術を積極的に習得し、日頃の業務において適切なセキュリティ対策を実践します。
- 特に、3D プリンターで製造するエンドエフェクタの設計データや、ノーコード GUI 等のソフトウェア資産を扱う際には、機密性・完全性・可用性を確保するための取り扱いを徹底します。

4. 法令及び契約上の要求事項の遵守

- 当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守し、お客様や研究機関の期待に応えます。
- 個人情報保護や産業スパイ行為などに関連する最新の法律・ガイドラインを把握し、適切に対応します。

5. 違反及び事故への対応

- 当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には速やかに事実関係を把握し、適切な対処を行います。
- 原因究明と再発防止策を講じ、これらを社内で共有し、同様の問題が再び発生しないよう継続的に取り組みを強化します。

6. 研究データおよびシステムへの配慮

- 当社は、ラボオートメーション導入先のお客様や研究機関から取得する実験プロトコルや研究データなど、機微な情報の保護を最重要課題の一つとして位置づけます。
- これらのデータの機密性・完全性・可用性を確保するため、適切なアクセス制御、暗号化、バックアップ等の技術的施策と運用ルールを導入・遵守します。
- システム稼働やソフトウェアアップデートにおいても、情報漏えいリスクを考慮し、セキュリティパッチ適用や運用プロセスの見直し等を的確に実施します。

7. リスク評価と継続的改善

- 当社は、情報資産に対して定期的なリスクアセスメントを実施し、脅威や脆弱性を把握するとともに、管理策の効果性を評価します。
- リスク評価の結果をもとに、当社の実情に合った対策を計画・実行し、PDCA（Plan-Do-Check-Act）サイクルを通じて情報セキュリティマネジメントを継続的に改善します。

8. 定期監査と見直し

- 当社は、情報セキュリティ対策の適切性および運用状況を確認するため、定期的に内部監査または第三者監査を行います。
- 監査結果やセキュリティインシデントの状況を踏まえ、基本方針や規程類を適宜見直すことで、情報セキュリティ体制の維持・向上を図ります。

制定日：2025 年 2 月 15 日

株式会社 QueeenB

代表取締役社長　根本一希