製品セキュリティポリシー

1. 基本方針

株式会社日立ハイテクおよび日立ハイテクグループ会社（以下、総称して当社）は、製品およびサービスの品質の一部としてサイバーセキュリティを重要な要素と位置づけ、製品の企画、設計、開発、提供、保守に至るライフサイクル全体を通じて、適切な製品セキュリティ確保に取り組みます。

当社は、製品の機密性・完全性・可用性を損なうサイバーリスクを低減し、お客様が製品を安全に利用できる環境の維持に努めます。

2. 法令・規格の遵守

当社は、製品セキュリティに関して、関連する各国・地域の法令および業界標準を遵守します。
あわせて、以下の国際的に認知された考え方や規格を参考に、継続的な改善を行います。

ISO/IEC 29147（脆弱性開示）
ISO/IEC 30111（脆弱性取扱い）

また、当社は EU Cyber Resilience Act（CRA）を含む製品に関するサイバーセキュリティ規制の動向を踏まえ、必要な体制および運用の整備を進めています。

Hitachi High-Tech Corporation
株式会社 日立ハイテク

3. 製品開発・品質への取り組み

当社は、製品設計および開発の段階から、サイバーセキュリティリスクを考慮した製品開発を行います。

設計時におけるリスクの識別・検討
適切な設計・実装・検証プロセスの適用
製品の用途および利用環境を考慮した対策

これらを通じて、製品に起因するセキュリティリスクの低減を図ります。

4. 脆弱性およびインシデントへの対応

当社は、自社製品に関する脆弱性やセキュリティ上の問題を把握した場合、適切な評価および是正対応を行います。

報告された脆弱性の内容確認・影響評価
是正策または緩和策の検討・実施
必要に応じた情報共有および公表

特に、製品の安全な利用に影響を及ぼすおそれがある場合には、利用者が適切な判断・対応を行えるよう、必要な情報の提供に努めます。

5. 脆弱性情報の受付と情報公開

当社は、外部からの善意の脆弱性報告を重要な情報源として受け止め、適切な窓口を設けて対応します。

また、脆弱性対応に関する情報については、早期警戒パートナーシップおよび協調的開示（Coordinated Vulnerability Disclosure）の考え方に基づき、製品の安全確保および利用者保護の観点から、関係者と連携のうえ、適切な範囲および時期で公開することがあります。

当社は、修正版の提供状況や利用者が取るべき対策について、可能な限り分かりやすい情報提供を行います。

6. 継続的な改善

当社は、脅威動向や技術進展を踏まえ、製品セキュリティに関する体制および取り組みを定期的に見直し、継続的な改善を行います。

これにより、製品の信頼性向上とお客様の安心・安全に貢献します。

Hitachi High-Tech Corporation

株式会社 日立ハイテク