セキュリティ脆弱性対応について

PSIRT（Product Security Incident Response Team）について

当社は、販売する半導体、通信端末、クラウド接続機器に関するセキュリティ脆弱性に対応するため、PSIRT（Product Security Incident Response Team）を設置いたしました。
セキュリティ脆弱性の報告、ならびにこれに関するご相談をお受けする体制を整備いたしましたので、お知らせいたします。

当社のセキュリティ脆弱性対応方針

基本姿勢

- 顧客保護の優先　：セキュリティ脆弱性の迅速な情報提供と対応支援
- メーカーとの連携　：製品開発元との協力による問題解決
- 透明性の確保　：対応状況の可能な限りの情報公開
- 継続的な改善　：セキュリティ対応体制の継続的向上

対応範囲

当社が販売する以下の製品に関するセキュリティ脆弱性に対応いたします。

- 半導体製品
- 通信端末
- クラウド接続機器
- その他

対応内容

1. 脆弱性情報の収集・分析
   - 各製造メーカーのセキュリティ情報の定期的な監視

2. 顧客への情報提供
   - 当社販売製品に影響を及ぼすセキュリティ脆弱性の検出時に顧客へ通知
   - 対策方法（パッチ、回避策等）に関する情報提供
3. 対応支援
   - 脆弱性対策の実施に関する支援
   - メーカー対応状況の説明

脆弱性報告窓口

報告方法

セキュリティ脆弱性の報告、およびセキュリティに関するご相談は、以下窓口までお願い致します。
メールアドレス：PSIRT@mizuho-ki.co.jp

報告時の情報

脆弱性報告の際は、可能な限り以下の情報をお知らせください。

- 対象製品名・型番
- 脆弱性の詳細（現象、影響範囲等）
- 発見時期
- 現在の対応状況

- ご連絡先（企業名、部門、氏名、メールアドレス、電話番号）

報告時の注意事項

- 脆弱性情報は機密情報として厳重に管理いたします。
- 報告いただいた内容は、当社およびメーカーの対応に限定して使用いたします
- 報告内容への回答に時間をいただく場合があります
- 脆弱性の重要度に応じて、対応優先度を決定させていただきます

当社PSIRT体制

当社では以下の体制でセキュリティ脆弱性に対応いたします。

組織体制

組織体制は経営企画部を中心に各営業本部、情報システム部、SCM本部で連携して対応します。

対応プロセス

1. 脆弱性情報の収集・確認
2. 当社販売製品への影響範囲の確認
3. 対策方法の検討・メーカーとの確認
4. 該当顧客への通知
5. 対応状況のフォローアップ

プライバシーと機密情報の保護

報告いただいたセキュリティ脆弱性に関する情報は、当社「個人情報保護方針」に基づいて、厳重に管理いたします。
報告者の氏名、組織名等の情報は、報告者の同意なしに第三者に開示することはございません。

最終更新日：2026年9月1日