

## サイバーセキュリティへの取り組み

### 基本方針

当社は、お客様に安全・安心な製品をご提供するため、品質、安全性およびサイバーセキュリティを重要な品質要素として位置付けています。

製品の企画・設計・開発・製造・保守・運用に至るライフサイクル全体を通じて、製品セキュリティの向上に取り組み、お客様に安心してご使用いただける製品の提供に努めます。

### PSIRT の設置

当社は、製品セキュリティに関するインシデントへ迅速かつ適切に対応するため、PSIRT(Product Security Incident Response Team)を設置しています。

PSIRT は、製品の脆弱性情報の受付、評価、対応および情報提供を行い、お客様への影響を最小限に抑える活動を実施します。

製品セキュリティに関する詳細は、「PSIRT」および「脆弱性開示ポリシー」をご覧ください。

## PSIRT(Product Security Incident Response Team)

### PSIRT について

PSIRT は、当社製品のサイバーセキュリティに関する情報を一元的に管理し、適切な対応を行うための組織です。

製品に関する脆弱性情報を受け付け、技術的な調査・影響評価を行い、必要に応じて開発部門、品質保証部門、製造部門などと連携して対策を実施します。

### 主な活動

PSIRT は、次の活動を行います。

- ・製品セキュリティ情報の収集
- ・脆弱性情報の受付
- ・技術的な調査およびリスク評価
- ・対策の立案・実施
- ・必要に応じたお客様への情報提供
- ・関係機関との連携

### お問い合わせ

製品セキュリティに関するお問い合わせは、脆弱性開示ポリシーに記載の受付窓口までご連絡ください。



## 脆弱性開示ポリシー(Coordinated Vulnerability Disclosure Policy)

### 基本方針

当社は、製品のセキュリティ向上のため、製品に関する脆弱性情報のご提供を歓迎します。  
ご報告いただいた内容は、適切に管理し、調査・評価を行ったうえで、必要な対策を実施します。

### ご報告いただきたい内容

可能な範囲で以下の情報をご提供ください。

- ・会社名・団体名 ※
- ・部署名
- ・お名前(フリガナ) ※
- ・E メールアドレス ※
- ・対象製品名 ※
- ・型式・ソフトウェア／ファームウェアバージョン
- ・脆弱性の内容(再現方法、想定される影響など) ※

※は必須項目

### ご報告方法

以下の専用窓口まで電子メールでご連絡ください。

E-mail: [psirt-info@inet1.aichitokei.co.jp](mailto:psirt-info@inet1.aichitokei.co.jp)

### 当社の対応

ご報告いただいた情報については、以下の手順で対応します。

- ・受付確認
- ・内容の調査
- ・影響評価
- ・必要に応じた対策の実施
- ・必要に応じた情報公開

なお、調査には一定の期間を要する場合があります。土曜、日曜、祝日、年末年始休暇、夏季休暇期間などにおいては、翌営業日以降のご対応となる場合があります。

### ご協力をお願い

製品をご利用中のお客様への影響を最小限とするため、当社による対応が完了するまで、脆弱性情報の公開はお控えいただきますようお願いいたします。

### 個人情報について

ご提供いただいた個人情報は、脆弱性対応以外の目的には使用いたしません。