脆弱性開示ポリシー

2025 年 12 月 1 日
Goal connect 株式会社
代表取締役　大下　明

当社は、IoT 製品のセキュリティ確保を目的に、外部関係者から当社 IoT 製品に関する脆弱性の報告を受理しております。報告を受領した場合は、以下の方針に則り、必要に応じて迅速かつ適切に対応いたします。

「脆弱性」とは、当社 IoT 製品に関するプログラムの不具合や設計ミスが原因となって発生した情報セキュリティ上の欠陥を指します。製品自体の破損や物理的な不具合は含まれません。

■ 対象範囲

当社が提供するすべての IoT 製品および関連サービス。

■ 報告方法

当社が提供する IoT 製品もしくは関連サービスにおける脆弱性の可能性がある事象を発見された場合は、下記の情報を明記のうえ、セキュリティ担当窓口へご連絡ください。

- セキュリティ連絡窓口：gc-isms@goal-connect.com
  ※対応時間：平日 9:00～18:00（日本時間）
- 必要情報：
  - 報告者様情報（任意：会社名、氏名、連絡先メールアドレスなど）
  - 対象製品情報（製品名、バージョンなど）
  - 脆弱性の詳細（具体的な内容、発生条件、再現手順、影響範囲など）
  - 証拠資料（スクリーンショット、ログファイルなど）
- 個人情報の保護について
  当社は、当社ホームページに掲載されている「個人情報保護方針」に基づき、報告者様からお預かりした個人情報を適切かつ厳正な管理のもとでその責務を履行いたします。
  また、報告者様が当社「セキュリティ連絡窓口」宛に脆弱性情報を送信された場合、当社の個人情報保護方針に同意いただいたものとして取り扱います。
  - Goal connect 株式会社 HP：https://www.goal-connect.com/

■ 報告受領後の対応方針

当社は、脆弱性の報告を受領後、原則 3 営業日以内に受領のご連絡を行います。

報告内容の再現および影響評価を実施し、必要に応じて技術的または運用上の是正措置を講じます。また、報告者の意見を聴取のうえ、適切な時期に情報を公開する場合があります。

■ 報告者の保護

当社は、善意かつ責任ある方法で脆弱性をご報告いただいた方に対し、法的措置を講じることはありません。ただし、悪意のある行為、または本ポリシーやその他の適用されるポリシーや法律に違反する行為は、適切な措置を講じる場合がございます。

■ 免責事項

本ポリシーに基づく対応は当社の管理体制に準じて実施され、内容は予告なく変更される場合があります。

以上