SECOM Sights 製品セキュリティに関する取り組みについて

セコム株式会社

2025.03.14 第 1 版

当社では SECOM Sights において、以下の方針の下、製品セキュリティの確保に取り組みます。

1. 製品セキュリティを確保するための体制を整備します。
2. セキュリティを考慮した設計・開発を行い、製品出荷前は、脆弱性検査により脆弱性の解消に努めます。
3. 製品出荷後も脆弱性情報を広く収集し、リスクがあると判断した場合は迅速に対応を行います。
4. セキュリティに関する情報や対策方法を利用者の皆様に提供します。
5. 製品開発者及び公的機関、セキュリティコミュニティ等から脆弱性情報を収集し、深刻度の高い脆弱性から対処を行います。
6. セキュリティ上の問題が発生した場合、セキュリティアップデートによるサポートを行います。上記はサービスの利用契約期間内のサポートとなります。

製品セキュリティに対して以下のような対応体制をとっています。

7. 組織体制
   製品セキュリティを確保するため、セキュリティバイデザインによる開発体制、脆弱性情報の収集体制、各プロセスを迅速に実行するための組織体制を整備します。
8. 外部との連絡体制
   製品における脆弱性およびその疑いが発生した場合、関連する開発元やサービス利用を行っている運用元に対して連絡を行い協調して対応を行います。

脆弱性に関する報告等については以下の開示ポリシーを策定しています。

9. 脆弱性に関する報告の連絡先
   当社は製品の情報セキュリティ品質向上のために、社外のセキュリティ研究者や調整機関から製品の脆弱性に関する情報を収集しております。製品の脆弱性に関する情報は、調整機関へご連絡いただくか、以下のアドレスへご連絡ください。
   SECOM Sights カスタマーサポート <cs@mail.secomsights.com>
10. 報告受領後の手続き・タイムライン
    ご連絡いただいた製品の脆弱性に関する情報は、当該製品の設計・開発部門にて確認を行い、以下の 3 点が確認された場合には、新規の脆弱性であると判断し、確認後速やかにご報告者様に確認結果をご連絡いたします。なお、確認にあたり、必要に応じ

て追加の情報提供をお願いする場合があります。
(ア) 製品のセキュリティに影響のある問題であること
(イ) 再現性があること
(ウ) 未公開であること
対応が必要だと判断された脆弱性に対し、該当する関係部門・関係者と脆弱性情報の公開に向けた調整を行い、脆弱性対策が準備出来次第、公開します。公開される情報の中に攻撃コードやハッカーなどの攻撃者に有利となる情報を含まないようにします。

なお上記の脆弱性に関する取り組みは予告なく変更されることがあります。

以上