

製品セキュリティガイドライン

1. はじめに

1.1 目的

本書は、当社が製造する製袋機/スパウトインサータ機(以下「当社装置」)を安全に設置、設定、運用、保守及び廃棄するために、ユーザー及び管理者が実施すべき基本的なセキュリティ対策を示すことを目的としています。

1.2 対象者

本書は以下の担当者がセキュリティ対策を実施する場合に活用することを想定しています。

- 機械導入担当者
- 設備管理者
- 保守担当者
- IT/OT ネットワーク管理者
- 袋取りなどの作業担当者

1.3 適用範囲

本書は以下の当社装置や機能について適用します。

対象装置/製品

- 製袋機/スパウトインサータ機本体
- 操作盤/パネル及び HMI
- 制御装置(PC、PLC 等)
- 保守用 PC 又は接続端末
- 製袋機/スパウトインサータに接続されるネットワーク機器
- 保守用ソフトウェア

対象機能

- ネットワーク通信
- データ収集
- リモートメンテナンス
- ソフトウェア更新/アップデート

1.4 免責事項

本書に記載のセキュリティに関する内容は、当社が行った分析・検討の結果に基づいていません。

ユーザーの環境により適切なセキュリティ対策は異なるため、本書に記載の内容でユーザーの環境下での全てのセキュリティ被害の防止を保証するものではありません。

また、ユーザーが安全に使用するための基本事項を示すものであり、詳細なネットワーク設計、詳細な権限設計、又は社内運用ルールの全てを規定するものではありませんので、ユーザーご自身で環境に合った適切な対応の検討及び実施をお願いいたします。

2. 安全に使うための前提条件

当社装置は、単体の機能だけではなく、接続される環境を含めて適切に保護されていることで適切なサイバーセキュリティ対策が実現できます。

そのため、ユーザーにおかれましては以下の要件を満たす環境で当社装置をご使用ください

2.1 設置環境

- 対象者以外の第三者が容易に近づけない環境に設置する。
- 操作盤、制御盤、通信ポート、USB ポート等に対する物理的なアクセスを制限する。
- 制御盤の鍵、保守端末、設定用媒体は適切に管理する。

2.2 ネットワーク環境

- 当社装置を業務用 IT ネットワーク又はインターネットに直接接続しない。
- 当社装置のネットワークは、他の業務ネットワークと分離する。

2.3 運用体制

- 当社装置ごとに管理責任者を定める。
 - 設定変更、ソフトウェア更新、保守接続は、権限を持つ者だけが実施する。
 - 障害、異常通信、認証失敗等を確認した場合の連絡先及び対応手順を定める。
-

3. 保証期間

セキュリティに関する保証は検収日から5年間(5年後の同月日まで)になります。

保証期間内はセキュリティパッチ/ソフトアップデートの配布など、セキュリティ対応を実施いたします。

4. 主なセキュリティ機能

当社装置は以下のようなセキュリティ機能を搭載しており、適切に使用することで装置及びユーザーの資産を守ることができます。

ただし、装置の機種やオプションを含めた仕様により搭載される機能は異なります。

4.1 ユーザ認証、権限管理

操作又は設定変更を行うユーザを識別するための機能です。

権限のない利用者による操作や設定変更を防ぐために使用します。

ユーザ権限として「オペレータ」「保守員」「管理者」の3つを用意しております。

区分により、設定変更、保守機能、システム情報参照等へのアクセス及び実施可能な操作を制限することができます。

4.2 ログ記録

ログイン、製袋条件を含む設定変更、警報、異常、保守操作等を記録する機能です。

異常の調査、原因確認、不正な操作の早期検知に使用します。

4.3 信頼業界外との通信保護

制御装置、HMI、保守端末等との通信を保護する機能です。

不正な接続、パケット盗聴、改ざんのリスクを低減するために使用します。

4.4 設定保護

重要な設定値の変更制限、設定保存、バックアップ等の機能です。

誤設定又は不正変更による影響を低減するために使用します。

5. 初期設定時の注意事項

当社装置の導入直後の初期状態のまま運用してしまうと、セキュリティの脆弱性がある状態になるため、少なくとも以下の内容について実施してください。

5.1 初期アカウントの確認

- 初期状態で存在するアカウントを確認する。
- 不要な初期アカウントは無効化又は削除する。
- 初期パスワードが設定されている場合は、運用開始前に変更する。

5.2 パスワード設定

- 推測しやすい文字列を使用しない。
- 装置名、会社名、機種名、連番等をそのまま使用しない。
- 管理者アカウント、オペレータアカウント、保守員アカウントで同一パスワードを使用しない。

5.3 ネットワーク設定

- 必要な接続先だけを許可する。
- 運用に不要なポート又はプロトコルは使用しない。
- IP アドレス及び接続構成を管理者が把握できる状態にする。

5.4 バックアップ

- バックアップ媒体を安全に保管する場所を準備する。

6. 推奨設定

安全な運用のため、以下の設定を推奨します。

6.1 アカウント設定

- 共通アカウントの使用を避ける。
- 利用者ごとに識別可能なアカウントを使用する。

- 管理者権限は必要な者だけに付与する。

6.2 通信設定

- リモート保守は常時有効にせず、必要時のみ有効にする。
-

7. 日常運用の注意事項

当社装置の運用中は、少なくとも以下を継続して実施してください。

7.1 利用状況の確認

- 警報や異常メッセージを放置せず確認し、必要に応じて管理者に報告する。

7.2 記録の確認

- ログを定期的に確認する。
- 必要に応じてログを改ざんされない状態で保管する。
- 異常又は不審な操作が確認された場合は、管理者へ報告する。
- 意図しないログインや設定変更がないか確認する。
- 不審な接続、再起動、停止等がないか確認する。

7.3 設定変更管理

- 設定変更は、承認された手順に従って実施する。
- 変更前後の内容を記録する。
- 原因不明の設定変更が見つかった場合は、直ちに確認する。

7.4 外部媒体の取り扱い

- 当社が許可していない USB メモリ、SD カード、保守ツールを接続しない。
- 保守に用いる PC については、ユーザーの社内セキュリティルールに則った管理をされており、かつ、最新の OS アップデートが適応済みで最新の定義でウイルスチェックが実施済みなもののみ使用する。
- 外部媒体を使用する場合は、使用前に最新の定義でウイルスチェックを実施する。

7.5 異常時の対応

- 通常と異なる動作、想定外の画面表示、原因不明の停止等を確認した場合は、直ちに管理者へ連絡する。
 - 状況確認前に安易な初期化や再設定、当社装置の再起動を行わない。
 - 必要に応じて装置をネットワークから切り離す。
-

8. アカウント管理

当社装置で使用するアカウントについて、以下の内容を継続して実施してください。

8.1 アカウントの原則

- 利用者ごとに適切な権限を設定する。
- 必要最小限の権限だけを付与する。
- 管理者権限は必要な作業以外で使用しない。

8.2 アカウントの登録・変更・削除

- 新規利用者登録時は、役割に応じた権限を設定する。
- 異動、退職、担当変更時は、不要となったアカウントを速やかに削除する。
- 長期間使用していないアカウントは定期的に見直す。

8.3 パスワード管理

- パスワードを他者と共有しない。
- 紙へのメモ、装置付近での保管、推測しやすい形式での記録を避ける。
- 初期パスワード及び一時パスワードは速やかに変更する。
- 8文字以上、英字/数字/記号の全てを使うことを推奨する。

8.4 デフォルトアカウント

- デフォルトアカウントが存在する場合は、使用有無を確認する。
- 不要な場合は無効化する。
- 使用が必要な場合は、アカウント名又はパスワードを初期値のまま使用しない。

9. 更新・問い合わせ

当社装置及び装置に搭載した機器に関して、当社からセキュリティパッチもしくはソフトウェアアップデートを必要に応じて準備します。

更新管理の際や、脆弱性及びインシデントを発見時には、下記の内容を実施してください。

9.1 更新管理

- 当社から提供されるセキュリティ情報、更新情報、脆弱性情報を確認する。
- 更新の適用前に、対象機種、影響範囲、停止影響を確認する。
- 更新前に設定及び必要データをバックアップする。
- 更新後は正常動作を確認する。

9.2 問い合わせ及び報告

- セキュリティに関する問題を確認した場合は、ユーザーの社内管理者又は指定窓口へ速やかに報告する。
- 当社への報告が必要な場合は、機種名、発生日時、現象、影響範囲、実施済み対応を整理して連絡する。
- 不審な事象が発生した場合は、ログ及び関連情報を保全する。

9.3 脆弱性及びインシデント報告窓口の設置

脆弱性を発見した場合に迅速に報告できるように脆弱性報告窓口を設置しています。

https://*****

10.廃棄・譲渡時の注意事項

廃棄又は譲渡前に、削除可能な情報を削除してください。

10.1 運用終了時

- 保存されているネットワーク設定、接続先設定、認証情報、保守設定を確認する。
- 必要に応じて設定を初期化又は削除する。
- 必要なログ、設定、保守情報を適切に回収する。

10.2 廃棄時

- 記録媒体を含む部品に情報が残存する可能性を考慮する。
- 機器内に保存されている設定情報、運用情報、ログ情報が削除されていることを確認し、安全に廃棄する
- 初期化/削除できない場合は、装置内の該当機器について電氣的・物理的な破壊などの対策をとり、情報漏えい防止措置を講じる。

11. ユーザーと管理者の責任

管理者及びユーザーにおいて、下記の内容について責任を持って実施してください。

11.1 ユーザーの責任

- 許可された範囲でのみ装置を使用する。
- 不審な挙動、異常表示、認証異常を発見した場合は報告する。
- アカウント情報及び操作権限を適切に管理する。

11.2 管理者の責任

- アカウント、権限、設定変更、更新、ログ確認を適切に管理する。
- 2.安全に使うための前提条件が維持されていることを確認する。
- 問題発生時に、ユーザーの管理部門及び当社との連絡体制を維持する。

11.3 共通事項

- 利便性を理由にセキュリティ設定を無効化しない。
- 例外運用を行う場合は、管理者承認のもとで実施する。
- 本書に定めのない事項は、当社の指示に従う。

本書に関するお問い合わせは、本社及び最寄りの各拠点までご連絡ください。

●本社・工場

トタニ技研工業株式会社

〒601-8213 京都市南区久世中久世町 5-81

代表 TEL : (075) 933-7610、FAX : (075) 933-7602

e-mail: 2007gad@totani.co.jp

●中国工場

大连户谷技研工业有限公司

大连经济技术开发区生命二路 2 号

Phone: +86-411-8792-2338, +86-411-8792-2318, Fax: +86-411-8792-2198

e-mail: 2007gad@totani.co.jp

●海外子会社

Totani America, Inc.

1701 Mid Valley Dr.

De Pere, WI 54115

Phone: +1-920-632-7319, Fax: +1-920-632-7361

e-mail: sales@totaniamerica.com

Totani Europe GmbH

Bonnerstrasse 203b 40589

Düsseldorf, Germany

Phone: +49 (0)211-7407-970

e-mail: sales@totanieurope.com

Totani Asia Pacific Pte Ltd.

10 Anson Road #15-13 International Plaza Singapore 079903

Phone: +65-6220-2982, Fax: +65-6220-2982

e-mail: 2007gad@totani.co.jp