フィールドバスシステム／産業用IoTセキュリティ対策

産業用IoTの導入により工場内の様々な機器がネットワークにつながることで、サイバー攻撃等の新たな脅威に対応する必要があります。産業用IoTを守るために、IoT機器、ネットワーク、クラウド等も含めて多層的に対策（多層防御）することが重要です。
SMCは、以下の対策を検討することを推奨します。記載されている対策に関する詳細につきましては、各国、各機関組織が発行するセキュリティ対策の文書等を参照してください。

①インターネット等のパブリックネットワークに機器を接続しない。
- ・パブリックネットワークを介して機器やクラウド等にアクセスする必要がある場合は、VPNや専用回線等のセキュアな回線を使用する。
- ・オフィス等の情報系ネットワークと工場内の産業用IoTネットワークを接続しない。

②機器およびシステムへ外部からの脅威流入を防ぐためにファイアウォールを設置する。
- ・ネットワークの境界にルータやファイアウォールを設置し、必要最小限の通信だけを許可するように設定する。
- ・通信の常時接続が必要でない場合は、未使用時に通信機器の電源を切る等、回線を切断する。

③未使用の通信ポートは物理的にアクセスできないようにする、または、設定で無効化する。
- ・ネットワーク機器に不要な機器が接続されていないか、各ポートを定期的に確認する。
- ・ネットワーク機器の各種サービス（SSH、FTP、SFTP等）は、必要なサービスだけを稼働させるように設定する。
- ・無線LANおよびその他電波を利用する機器は伝搬範囲を適切に設定し、設置国の電波法認定を受けた適切な機器を使用する。
- ・無線電波を出力する機器は、屋内外から電波の干渉が無い場所へ設置する。

④データ暗号化などセキュリティ対策がなされた通信方式を設定する。
- ・IoTネットワークやセキュアなゲートウェイ経由の接続等それぞれの環境において、暗号機能によるセキュリティ対策を実施する。

⑤アカウント毎にアクセス権限を付与し、利用できるユーザを限定する。
- ・アカウントを定期的に見直し、使わなくなったアカウントや権限を削除する。
- ・ログインエラー回数が基準値を超えた場合には、そのアカウントを一定時間使用禁止にする等、アカウントロックの仕組みを設定する。

⑥パスワードを保護する。
- ・初期設定されていたパスワードは導入時に変更する。
- ・パスワードを定期的に変更する。
- ・パスワードは推測されにくく、安全性が高い組合せのパスワード（例えば文字や特殊文字を含んだ8文字以上）を設定する。

⑦最新のセキュリティソフトウェアを使用する
- ・ウイルス感染を検知・駆除するために、ウイルス対策ソフトウェアをすべてのPCに導入する。
- ・ウイルス対策ソフトウェアは常に最新の状態を維持する。

⑧機器およびシステムのソフトウェアは最新バージョンにする。
- ・OSおよびアプリケーション等が最新の状態になるようパッチを適用する。

⑨ネットワーク内の監視・異常検知をする。
- ・異常が発生した場合、迅速に対応するためにネットワーク内の通信を監視し、異常を検知した場合にアラートを通知する。侵入検知／防御システム（IDS/IPS）等の機器を導入する。

⑩機器の廃棄時や手放す時にデータ削除をする。
- ・IoT機器を廃棄する際に、機器に残されたデータを不正に利用されることを防ぐためにデータ削除や物理的な破壊を行う。