「工場における産業用 IoT 導入のためのセキュリティ ファーストステップ」

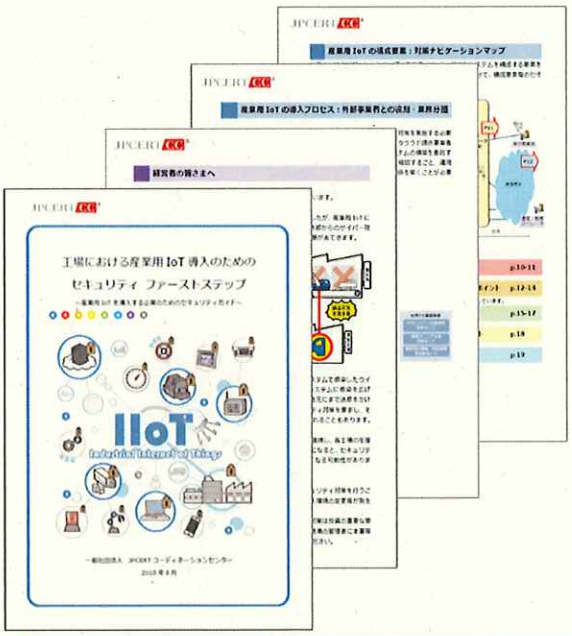
～ 製造現場でセキュアに産業用 IoT を活用するためのセキュリティ対策ガイド ～

ご案内

一般社団法人 JPCERT コーディネーションセンター
制御システムセキュリティ対策グループ

生産設備の稼働状況の見える化や故障予知、収集データの解析結果を活用した自動制御など、産業界でもさまざまな用途で IoT の活用がすすむ中、一方で産業用 IoT の導入により工場内のさまざま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出てきます。万一被害に遭うと自社の生産活動への影響のみならず、取引先などのサプライチェーン全体にまで影響を及ぼす恐れがあります。このため、そのような脅威へのセキュリティ対策を進めるための一助となるよう、一般社団法人 JPCERT/CC では「工場における産業用 IoT 導入のためのセキュリティ ファーストステップ」を公開いたしました。本資料は、「中小を含む製造業者」における「工場での IoT」の「導入時」にご利用いただけるよう、**IoT 機器を製造現場に導入する製造業の経営者や制御システムの現場担当者および設計や構築を担うエンジニアリング会社の方を対象としたセキュリティ対策ガイド**です。無料でご利用いただけます。

【公式 Web ページ】
工場における産業用 IoT 導入のためのセキュリティ ファーストステップ
https://www.jpcert.or.jp/ics/information06.html



本資料の主な構成（全 22 ページ）

1. **『経営者の皆さまへ』**
   - **経営者対象：**被害コストを例示しながら、必要なリソースの確保や指示等経営者の役割を解説
2. **『産業用 IoT のセキュリティ対策の考え方』**
   - **全読者対象：**セキュリティ対策に万全はないことを踏まえ、多層防御の重要性を解説
3. **『産業用 IoT の導入プロセス』**
   - **現場管理者・技術担当者対象：**ベンダとの責任分界や契約を含め、仕様策定から運用までの各プロセスで実施すべきセキュリティ対策の概要を解説
4. **『対策ナビゲーションマップ』**
   - **現場管理者・技術担当者・ベンダ・SIer 等対象：**対策ナビゲーションマップとして 5 つのパートで構成される産業用 IoT ネットワークモデルを図示し、それぞれのパートごとに対策の重要性と対策例を解説

【本書で得られる知識等】
・産業用 IoT の導入によるセキュリティリスク(想定されるリスク例など)
・セキュリティ対策を行う際の考え方(どのような視点で対策を行うべきか)
・産業用 IoT 導入時に実施すべき基本的なセキュリティ対策(具体的な対策例など)
・セキュリティ対策を行うための主な実施手順

【お問い合わせ】
一般社団法人 JPCERT コーディネーションセンター (制御システムセキュリティ対策グループ)
TEL:03-6271-8901／Email:icsr@jpcert.or.jp (担当：河野)