

# OTセキュリティポリシー ・OTガイドライン策定サービス

# INJANET

AI活用による短期間・高品質なOTセキュリティ  
文書を低料金で入手できます

## 📄 こんなお悩みはありませんか？

- OTセキュリティポリシー・OTセキュリティガイドラインをつくりたいが、何をどう書けばよいかわからない
- 国際規格（IEC 62443 等）準拠の文書を作りたいが社内に知識がない
- セキュリティ担当者が少なく、文書作成に時間をかけられない
- 監査・取引先からセキュリティポリシーの提出を求められている

## 💡 サービス概要

参照規格、お客様へのヒアリングを元に、AIを活用した効率的なプロセスで以下2つのOTセキュリティ文書を生成します。

### ① OTセキュリティポリシー（基本方針）

経営層向けのOTセキュリティの基本方針・宣言文書

### ② OTセキュリティガイドライン

現場担当者向けの具体的なセキュリティ対策基準・手順

Security

## 🔄 サービスの流れ（生成プロセス）

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
情報収集	規格参照	AI生成	専門家確認	完成・納品
既存ポリシー・ヒアリング・アンケート	IEC 62443 NIST CSF 2.0 経産省 GL 等	AIが草案を自動生成	INJANET 担当者が内容精査・修正	顧客フィードバックを経て最終完成

## 📖 参照する規格・標準（例）

- IEC 62443-2（産業制御システムセキュリティ）
- NIST CSF 2.0（サイバーセキュリティフレームワーク）
- CIS Controls V8
- CISA Cross Sector CPGs
- 経産省 CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）
- 経産省 工場システムサイバー・フィジカル・セキュリティ対策 GL
- 自工会/部工会 サイバーセキュリティガイドライン 等

## ★ INJANET を選ぶ理由

- IPA「制御システムのセキュリティリスク分析」の講師・実務経験あり
- IT/OT 双方のセキュリティギャップを深く理解
- AI活用により短期間・低コストで高品質な文書を提供
- 人間の専門家が最終確認するため安心・信頼の品質保証

## 💰 料金目安・お問い合わせ

### 料金目安(税抜)

工場規模 ~100名 ~300名

- OTセキュリティポリシー策定： 18万円 48万円～
- OTセキュリティガイドライン作成 37万円 70万円～
- セットでのご依頼：割引対応あり
- 初回メール相談：無料

※規模・複雑さにより変動します。まずはお気軽にご相談ください。

### お問い合わせ

INJANET 株式会社

🌐 <https://injanet.co.jp>

Webサイトの【お問い合わせ】ページまたは上記メールアドレスよりご連絡ください。

## 【作成例】

### ●OTセキュリティポリシー（基本方針）

XXX グループ

# OTセキュリティ基本方針

OT Security Policy

XXX グループは、「企業は社会の公器」との基本理念のもと、工場・生産拠点および制御機器・産業用機械システムにおける OT (Operational Technology) 環境のサイバーセキュリティを経営上の重要課題と位置づけます。生産活動の継続性、安全、そして社会インフラの安定に貢献する責任を果たすため、以下の方針を定めます。

- 1 経営主導による OT セキュリティの推進**  
代表取締役社長 CEO を最高責任者とし、グループ全体の OT セキュリティ体制を整備・維持します。OT セキュリティを経営戦略の一部として継続的に推進し、必要なリソースを確保します。
- 2 OT 資産・環境の保護**  
工場・生産拠点における制御システム (PLC・SCADA・DCS 等) および OT ネットワークを対象に、リスクアセスメントを定期実施し、不正アクセス・マルウェア・設定改ざん等の脅威から保護します。
- 3 IT/OT ネットワークの分離と境界管理**

## 【作成例】

### ●OTセキュリティガイドライン

社外秘

XXX Group OT Security Guideline GL-01 / GL-02

## 1. はじめに

目的	本ガイドラインは、XXX グループの OT セキュリティ基本方針に基づき、工場・生産拠点の制御システム (PLC・SCADA・DCS 等) および OT ネットワークにおける具体的なセキュリティ対策手順を定めるものです。
背景	制御システムへのサイバー攻撃が世界的に増加しており、工場停止・設備破損・安全事故に直結するリスクが高まっています。本ガイドラインは IEC 62443・NIST CSF 2.0・CIS Controls の要求事項を XXX グループの環境に適用したものです。

## 2. 適用範囲

本ガイドラインは、XXX 株式会社および国内外グループ会社の下記環境に適用します。

- 工場・生産拠点内の OT ネットワーク (制御系 LAN・フィールドバス等)
- PLC・SCADA・DCS・HMI・エンジニアリングワークステーション等の制御機器
- IT/OT 境界に設置するファイアウォール・DMZ 等のセキュリティ機器
- 外部 (ベンダー・保守業者) が接続するリモートアクセス環境

## 3. 準拠規格

規格・ガイドライン	概要
IEC 62443-2-1 Ed.2	産業用オートメーション・制御システムのセキュリティ管理プログラム要求事項
NIST CSF 2.0	サイバーセキュリティフレームワーク (特定・保護・検知・対応・復旧・統治)
CIS Controls v8	インターネットセキュリティセンターが定める優先度付きセキュリティ対策集

INJANET 株式会社