

# 制御システム向け セキュリティ現状分析サービス

国際規格 IEC 62443 に基づいて  
制御システムのセキュリティをチェック！

近年、制御システムをとりまく技術やネットワークプロトコルなどの標準化が進む中、  
オフィスの情報ネットワークとの部分的な連携が増え、サイバー攻撃などの脅威にさらされています。

まずは、制御システムのセキュリティ規格として標準化されている  
IEC 62443 に基づいてセキュリティ要件をチェックすることから始めるのが効果的です。



## 専門知識がない

現状のセキュリティリスクや  
必要な対策がわからないため、  
的確なセキュリティ対策が  
できない可能性がある。

## 課題



## 時間やコストを かけられない



全てのシステムに、いきなり  
セキュリティ対策をしようとすると、  
時間やコストがかかり、  
現実的ではない。

## 日立ソリューションズの 制御システム向け セキュリティ現状分析サービスは

- 実施すべき対策ごとに点数化し、セキュリティレベルを診断
- 技術的対策だけでなく、組織的運用の対策状況も分析
- 診断結果を基に、推奨する対策も提案

### POINT 1

#### 国際規格に基づく診断

制御システムセキュリティの  
国際規格である IEC 62443  
に基づく診断です。



### POINT 2

#### 手軽に現状把握

工場の製造ラインやプラントの  
制御システムのセキュリティを  
ヒアリングベースで  
診断します。



### POINT 3

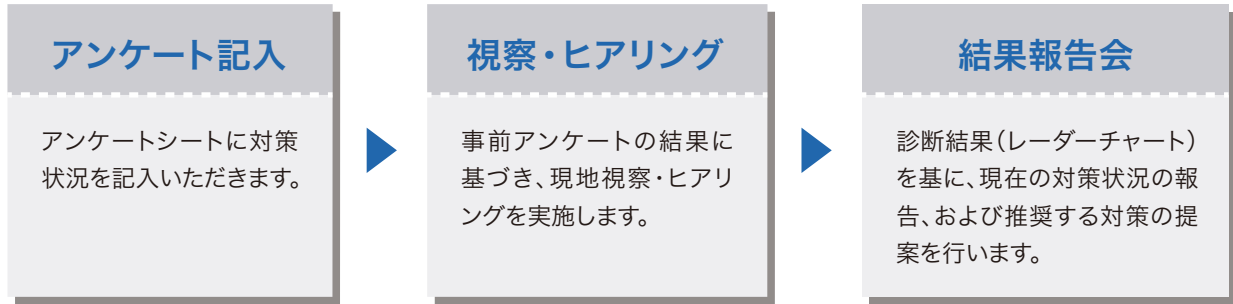
#### 低コスト

詳細分析の前に、  
どれだけ現状が危険なのかを  
低コストで  
診断できます。



## 診断の流れ

制御システムの現地視察とヒアリングを基に、診断を実施します。



### アンケート記入

アンケートシートに対策状況を記入いただきます。

### 視察・ヒアリング

事前アンケートの結果に基づき、現地視察・ヒアリングを実施します。

### 結果報告会

診断結果(レーダーチャート)を基に、現在の対策状況の報告、および推奨する対策の提案を行います。

## 診断項目

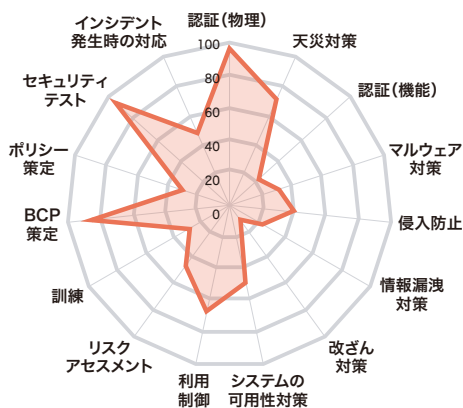
パスワードの設定やマルウェア対策などのセキュリティ機能面、組織的な運用面での対策状況も含めて可視化し、対策カテゴリーごとにセキュリティレベルを診断します。

対策カテゴリーの例	チェック内容
認証(物理)	装置や機器への物理的なアクセスを防御するための対策状況
認証(機能)	装置や機器へのログイン制限の状況
可用性対策	制御システムが動き続けるような機能的対策の状況
利用制御	USBやCD、モバイル機器などの接続に関する対策状況
マルウェア対策	PC・サーバーのマルウェア感染防止対策状況



## 診断結果イメージ

カテゴリーごとの評価や推奨対策を提示します。今後の対策検討にお役立てください。



15の対策カテゴリー

セキュリティレベルを100点満点で点数化

レーダーチャートでセキュリティ対策のレベルが一目瞭然

※本カタログ中の会社名、商品名は各社の商標、または登録商標です。※本文中および図中では、TMマーク、®マークは表記しておりません。※製品の仕様は、改良のため、予告なく変更する場合があります。※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。※本カタログ中の情報は、カタログ作成時点のものです。

◎ 株式会社 日立ソリューションズ

www.hitachi-solutions.co.jp



本カタログ掲載商品・サービスの詳細情報

www.hitachi-solutions.co.jp/security/sp/solution/task/seigyo-sec.html

S18K-13-01 2018.09