HITACHI
Inspire the Next

制御システムセキュリティソリューション

株式会社 日立ソリューションズ

制御システムのセキュリティ課題

- ☑ 制御システムのセキュリティを強化したいが、何から対策していいかわからない。
- ☑ 制御端末は、動作アプリケーションの影響によりレガシーOSで動作している場合が多く、セキュリティを組み込むことが困難なため、セキュリティ対策が取れない。
- ☑ 現場計器の異常（温度上昇など）が発生しても、通常の操作ミス・装置の故障などが原因なのか、サイバー攻撃が原因なのか判断が難しく、対策が遅れてしまう。

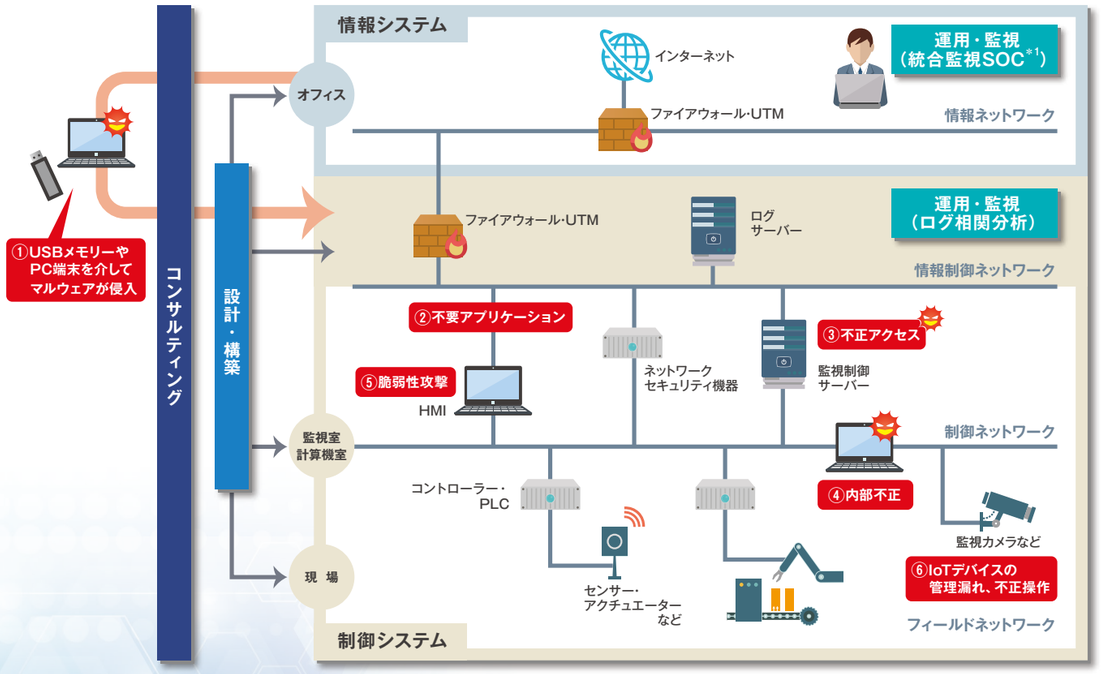
守る 日立ソリューションズにお任せください

日立ソリューションズは、お客様の制御システムに必要なセキュリティ要件を整理し、現在稼働している制御装置、制御端末に影響を与えない形で効果的な対策を提供します。

必要なのは、可用性を重視したセキュリティ対策。

近年、制御システムは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、一般的なセキュリティリスクの脅威にさらされています。
制御システムでは可用性が最優先され、24時間365日の稼働が求められること からも、システムへの影響を抑えた対策を施す工夫が求められています。

制御システムセキュリティの脅威と対策



	脅　威	対　策
①	USBメモリーやPCを介したマルウェアの侵入	USBメモリーやPCのマルウェア検知・防御
②	不要なアプリケーション利用による情報漏洩	ホワイトリストによるアプリケーション利用制御
③	ネットワークからの不正アクセス、マルウェア侵入	一方向通信制御、不正侵入検知・防御
④	内部不正	不正端末接続防止、生体認証やICカードなどによる端末認証強化
⑤	HMI*2、PLC*3ソフトウェアの脆弱性を突いた攻撃	不正侵入検知・防御
⑥	IoTデバイスの管理漏れ、不正操作	IoTデバイス管理

*1 SOC（Security Operation Center）：セキュリティ・サービスおよびセキュリティ監視を提供するセンター
*2 HMI（Human Machine Interface）：人間と機械が情報をやり取りするための手段や、そのための装置やソフトウェア
*3 PLC（Programmable Logic Controller）：シーケンス制御専用マイクロコンピュータ

さまざまな対策で、セキュリティリスクから制御システムを守ります。

ソリューションの特長

業界ガイドラインに精通したコンサルタントによる、課題に応じた効果的な対策を提案

制御システム特有のセキュリティ要件や、業界ガイドライン（NERC CIP*4、IEC62443*5など）に精通するコンサルタントが、セキュリティリスクを分析し、課題に応じた効果的な対策を提案します。

*4 NERC CIP：NERC（北米電力信頼度協議会）により発行された重要インフラストラクチャを保護するための強制的な基準
*5 IEC62443：汎用的な制御システムのセキュリティについて、事業者による管理運用をはじめ、技術、システム、デバイスまで包括的に規定した国際規格

稼働中のシステムへの影響を抑えた、可用性重視のセキュリティ対策を実施

制御システムの可用性を重視し、セキュリティパッチやシグネチャの更新が不要となるホワイトリスト方式のセキュリティソリューションや不正アクセス検知など、システムへの影響を抑えた適切なセキュリティ対策を幅広く提供します。

自社・日立グループ製品などを組み合わせ、計画から設計・構築、運用・監視までトータルに支援

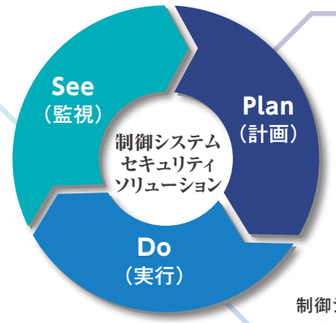
豊富な自社・アライアンス製品ならびに日立グループの製品群を組み合わせて、コンサルティングから設計・構築、運用・監視まで、効果的なソリューションをワンストップで提供します。

ソリューション概要

制御システムの継続的で安定的な稼働を実現

制御システムセキュリティ
運用・監視サービス

制御システムのログを相関分析することで全体のセキュリティ状態を認識するSIEM*6や不正アクセス監視により、制御システム異常の早期発見、早期原因把握を実現します。



制御システムセキュリティ
コンサルティング

特定業種向けのセキュリティコンサルティングのノウハウを活用し、現状分析サービス、脆弱性診断など、お客様の制御システムセキュリティ対策における現状の課題を明確にし、マネジメントとシステムの両面でセキュリティ強化を支援します。

制御システムセキュリティ
設計・構築サービス

レガシーOSに対応したホワイトリスト方式製品の導入による対策など、お客様のニーズに合った効果的なシステムを提案し、構築を支援します。

*6 SIEM（Security Information and Event Management）：サーバーやネットワーク機器、セキュリティ関連機器、各種アプリケーションから集められたログ情報に基づいて、異常があった場合に管理者に通知したり、その対策方法を知らせたりする仕組み

製品・サービス一覧

ソリューション区分	対 象	対 策	概 要
制御システムセキュリティコンサルティング	システム全体	セキュリティ現状分析	制御システム特有の環境を考慮した独自の手法を用いて、現地視察やヒアリングにより現状の脅威・リスクを分析し、改善案を提示
		サプライチェーンセキュリティ評価	取引先におけるセキュリティ対策状況の評価代行や改善案の提示、国際的な規格・基準をベースにした評価基準の作成支援を実施
		脆弱性診断	組み込み機器など個別アプリケーションの通信に存在する脆弱性や、不正侵入時に利用される脆弱性の有無を独自の診断ツールを用いて診断
		ペネトレーションテスト	脆弱性に対し、段階的な侵入を想定した脅威シナリオに沿って専任技術者が疑似攻撃を実施。セキュリティ強度を評価し、課題を見える化
制御システムセキュリティ設計・構築サービス	ネットワーク	一方向通信制御	情報公開先を経由した不正アクセスおよびマルウェアの侵入を物理的に遮断することにより、制御システムを保護
		ホワイトリスト方式 不正侵入検知・遮断	ホワイトリスト機能付きスイッチに置き換えるだけで、サイバー攻撃や不正端末による接続など不審な通信をシャットアウト
		シグネチャ方式 不正侵入防御	ネットワークを流れるパケットを監視し、不正アクセスなどの異常通信を監視。制御系プロトコルや温度差、粉塵などの過酷な環境にも対応
		振る舞い検知方式 マルウェア対策	Web経由のマルウェア感染・脆弱性を突く攻撃など、不正通信を監視しブロック
		不正端末接続防止	未登録PCや不正ユーザーによる社内ネットワークへの不正接続を検知し、接続を阻止
		IoTデバイス管理	IoTデバイスを自動で識別し、データベース化。MACアドレス、ベンダー、OSなど詳細情報の管理や異常動作時のアラート表示が可能
	HMI端末	ホワイトリスト方式 マルウェア対策	定義ファイルの更新が困難な制御端末では、あらかじめ起動を許可するアプリケーションを登録し、マルウェアなど未許可アプリケーションの実行を禁止
		エンドポイント型 マルウェア対策	従来型のアンチウイルスソフトウェアとは異なり、定義ファイルに依存せず、既知・未知のマルウェアや脆弱性攻撃を防御
		HMI端末認証強化	HMIなどの制御端末や生産管理サーバーへのなりすましによる不正ログインを防止し、生産ライン全体のセキュリティを強化
		USB制御	未登録USBメモリーの接続を禁止し、適切な利用を徹底。OSに依存せず、既存システムに影響を与えないため容易に導入可能
	システム全体	セキュリティログ相関分析システム構築	各システムのログを集約し、サイバー攻撃や不審行動を監視する統合ログ分析システムを構築
制御システムセキュリティ運用・監視サービス	システム全体	セキュリティログ相関分析	多種多様なログを相関分析することで、制御システム全体のセキュリティ状態を把握し、システム異常に対する対策を実現
		セキュリティ統合監視（SOC）	制御システムへのサイバー攻撃や内部不正などのログを一元的に収集・分析し、セキュリティ異常の早期発見・早期対策を実現

※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

S15S-13-03 | 2022.07