

2018年6月28日

報道担当各位

株式会社シーイーシー

工場をセキュリティ脅威から守るソリューション 「SecureCross™ Factory」を提供開始

株式会社シーイーシー（本社：東京都渋谷区、代表取締役社長：田原 富士夫、以下 シーイーシー）は、工場のスマート化やIoT（Internet of Things）活用におけるセキュリティ課題を解決するソリューション「SecureCross Factory（セキュアクロス ファクトリー）」を本日より提供開始します。

SecureCross Factoryは、工場で起こりうるセキュリティ被害や脆弱性に対応する、環境やエリア特性に適したソリューションです。生産設備がつながる工場IoT、制御システムなど「生産エリア」に特化したセキュリティソリューションから順次提供します。

■背景

工場では、独自のOSや通信プロトコルをベースとした制御システムが普及しています。近年は、システムコストの低減および相互運用性の向上を目的としたオープン化^{※1}、IoTの普及、グローバル拠点に広がるスマートファクトリーの実現に向けたネットワーク接続が欠かせなくなり、サイバー攻撃による重大な被害も年々拡大しています。

※1「オープン化」：WindowsやLinuxなどの汎用OS、EthernetやTCP/IPなどの標準プロトコルの採用

＜工場を取り巻くさまざまな脅威と被害＞

- 制御システムのウイルス感染（生産ラインの停止）
- 情報ネットワーク・制御システムへの不正侵入（設備故障）
- 不正侵入者による情報窃取、内部不正による情報の持ち出し（情報流出）

そこで、シーイーシーは、生産現場のデジタル化と自動化に強みを持つスマートファクトリー領域の知見、IT・OT（Operational Technology）機器のセキュリティ評価・認証支援、サイバーセキュリティマネジメントシステムにおけるガイドラインに準拠した運用など、長年培ってきたセキュリティ技術を融合しました。

■「SecureCross Factory」の概要

SecureCross Factoryは、工場で守るべき資産（情報、データを含む）やその重要度に着目した「4つのエリア」を定義し、それぞれのエリアに適したセキュリティ対策（サイバーセキュリティ対策・物理セキュリティ対策・人的セキュリティ対策）を提供します。



詳しくは：https://security.cec-ltd.co.jp/securecross_factory/

<各エリアの脅威とセキュリティ対策>

【1】「生産エリア」

「生産エリア」は、工場の基幹となる生産設備を収容した生産ラインの建屋を対象としています。ネットワークを経由したウイルス感染やサイバー攻撃による生産設備・制御システムの被害を防ぎます。工場内への不正侵入や製品・部品・原材料・図面・機密データの不正流出を防ぐ、入退室管理、映像監視など各種対策を提供します。

【2】「専有エリア」

「専有エリア」は、開発部門、製造部門の事務棟（オフィスエリア）を対象としています。外部からの不正侵入による情報窃取、標的型メール攻撃による情報漏えいやランサムウェアによるシステム・サービスの停止を防ぐ、入退室管理、映像監視、オフィスセキュリティ対策を提供します。

【3】「共有エリア」

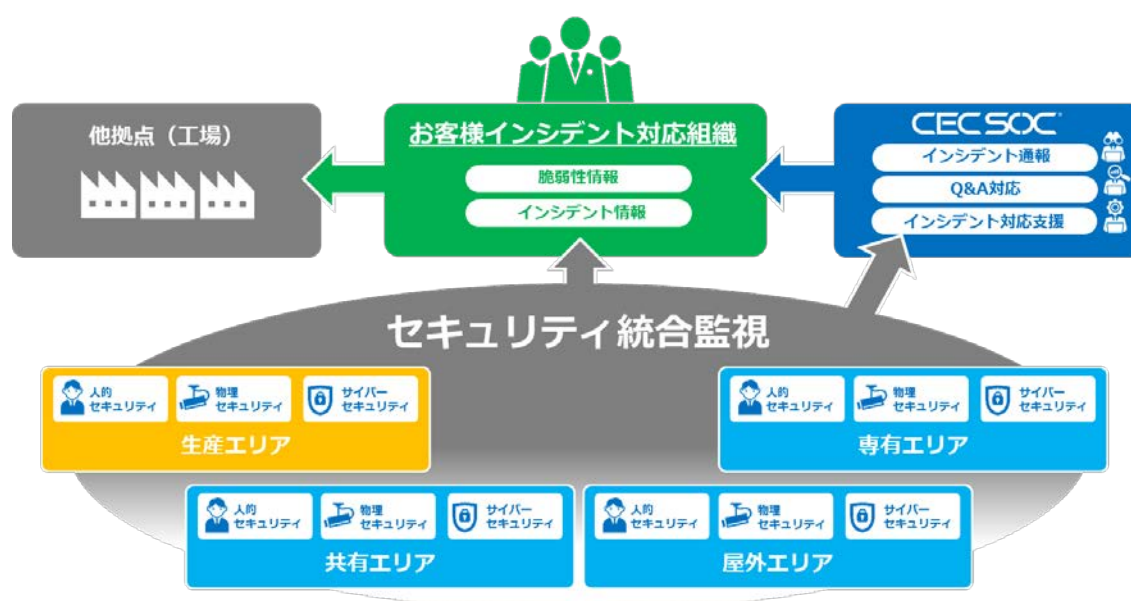
「共有エリア」は、エントランス（受付、会議室など）を対象としています。外部からの不正侵入による情報窃取、不正なネットワークアクセスによる情報漏えいなどを防ぐ、入退室管理、映像監視、オフィスセキュリティ対策を提供します。

【4】「屋外エリア」

「屋外エリア」は、工場の外周、駐車場、入出荷所などを対象としています。外部からの不正侵入による製品や原材料などの盗難を防ぐ、外周センサー（侵入者監視）、車両入退管理、映像監視の対策を提供します。

【5】「統合監視」

上記4つのエリアの各種イベントやシステムログ、アラート情報を集約し、工場全体の「セキュリティ脅威の可視化」を実現する「セキュリティ統合監視」と「CEC SOC[®]」※2によるセキュリティ監視・分析、インシデント対応の支援にて、予防保全と被害損失を最小限に抑える仕組みを提供します。※2「CEC SOC[®]」：専門家による24時間365日のセキュリティ監視・対処支援サービス



図：SecureCross Factoryの全体イメージ

■今回提供を開始するセキュリティ対策メニュー

＜各エリア共通のセキュリティ対策サービス＞

各エリアに共通するコンサルティング、教育・アドバイザーサービスを提供します。

エリア区分	管理区分	対策サービス	概要
共通	コンサルティング		
		アセスメント	リスクの特定、分析、評価による工場のセキュリティ対策状況の可視化
		セキュリティポリシー策定支援	アセスメントに基づく実施基準の策定（ドキュメント作成支援他）
	教育・アドバイザー		
		セキュリティ対策組織の構築（CSIRT構築）	インシデント対応における体制構築支援
	セキュリティ教育（セキュリティ専門家の育成）	現場作業や管理者向けのセキュリティ教育	

＜「生産エリア」のセキュリティ対策サービス＞

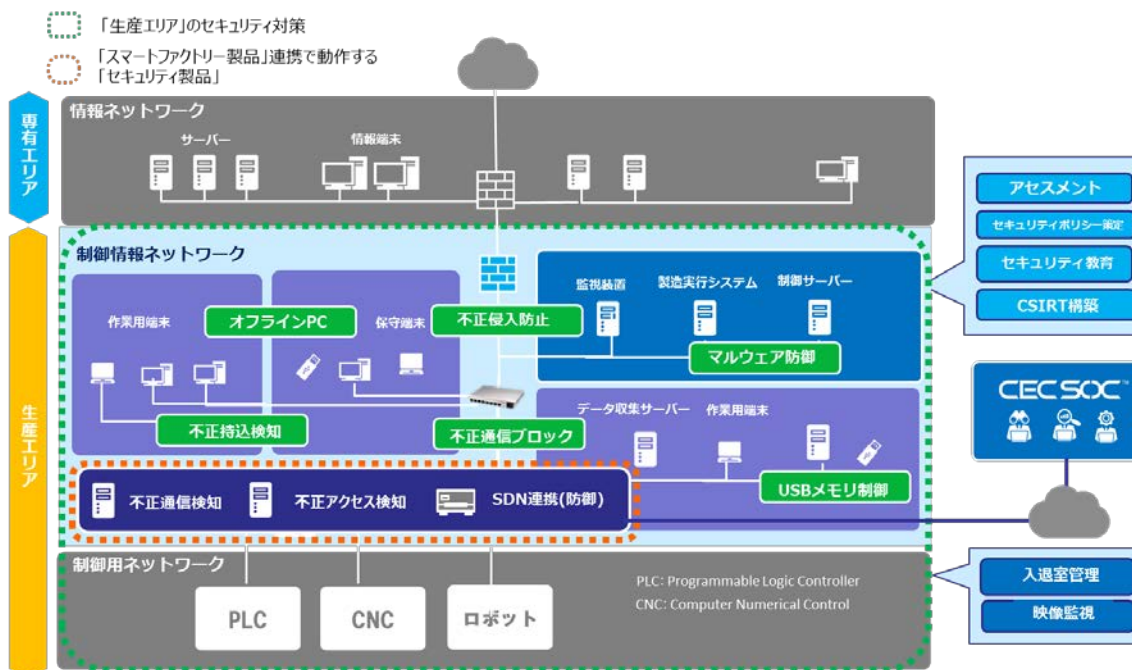
エリア区分	管理区分	対策サービス	概要
生産エリア	入退室		
		入退室管理システム	用途に合わせた通行制御と在室管理、映像監視システム連携
	映像		
		映像監視システム	利用シーンや環境に合わせた映像監視、入退室管理システム連携
	制御システム セキュリティ製品への実装		
		不正侵入防止	情報ネットワークと制御用ネットワークの分離 不正アクセスの検知・遮断、ネットワーク通信監視（分析）
		不正通信ブロック	制御装置、サーバー、PC間の必要な通信のみを許可
		不正通信検知 ●	ネットワークセンサーによる不審な通信検知（CEC SOCによる監視、対処支援）
		不正持込検知	持ち込みPCの検疫（ネットワーク接続の検知、遮断）
		不正アクセス検知 ●	生産設備への不正アクセス、プログラム改変検知
	マルウェア防御	制御用サーバー、制御用PC等のマルウェア対策、最新性維持	
	オフラインPC	オフラインPC、OSの保守切れPC対応（アプリケーションコントロール）	
	USBメモリ制御	USBメモリの利用制限、ウイルス感染防止（検知・駆除）	
	SDN連携（防御） ●	SDN連携によるネットワークの切り離し	

工場の生産設備を収容した「生産エリア」を対象に、①情報ネットワークと制御用ネットワークの分離、②生産設備とつながるネットワークの不正通信を検知・防御する仕組み、③マルウェア対策などの多層防御を軸に、可用性・完全性・機密性の高いセキュリティ対策を実現します。

シーイーシーは、生産ラインの可視化、稼働監視・稼働実績管理システムの構築や工場内のデータ収集に熟知し、国内主要メーカーの産業用ロボット、FA 機器・加工機・数値制御装置（CNC）の設計、配線、各種設定など組立・加工現場で培った高度なノウハウを活かし、工場のセキュリティ対策を支援します。

上記対策（●印）は、シーイーシーが提供する「スマートファクトリー製品」と今後連携し、「設備状況の可視化」に加え「セキュリティ脅威の検知と防御」※3を実現します。

※3 「セキュリティ脅威の検知と防御」：ネットワークセンシングによる制御情報ネットワーク内の「不正通信検知」、生産設備からの情報取得による「不正アクセス検知」、SDN（Software Defined Network）連携による異常検知時の「防御（ネットワークの切り離し）」



図：「生産エリア」の各種対策を含めた構成イメージ

■各エリアのセキュリティ対策サービスの提供について

「生産エリア」に続く各種対策サービスは、セキュリティ製品メーカーや物理セキュリティメーカー各社との協業を推進し、2018 年秋以降より順次提供します。

■販売目標

シーイーシーが提供する「スマートファクトリー製品」導入済みのお客様をはじめ、2020 年までに国内 100 社への販売を目標とします。

■この資料に関する問合せ先

【取扱事業部門・照会先】

株式会社シーイーシー【担当：デジタルインダストリービジネスグループ 第一営業部 下川（沓カ）】
〒150-0022 東京都渋谷区恵比寿南 1-5-5 JR 恵比寿ビル
Tel : 03-5789-2442 E-mail : marketing@cec-ltd.co.jp

【報道関係者問合せ先】

株式会社 シーイーシー【担当：事業推進本部 企画部 広報グループ 根本（社）】
〒150-0022 東京都渋谷区恵比寿南 1-5-5 JR 恵比寿ビル
Tel : 03-5789-2442 E-mail : kouhou@cec-ltd.co.jp

※ 記載の会社名・商品名等の固有名詞は各社の商標又は登録商標です。

以上