工場／医療現場での IoT化による脅威

～ 産業機器・医療機器の安全確保 ～

アドソル日進株式会社
IoTソリューション事業部
セキュリティ・ソリューション部
緒方 洋敬

ژ ڃ ڳ ف

01

市場動向

IoTデバイスの急速な普及

02

サイバー攻撃の脅威（インシデント）

工場のデジタル化でサイバー攻撃の標的に

2017 WannaCry

- 「Wa… ランサムウェアが世界…国以上で猛威を振るう
- 仏ル… …／日立製作所
  などで甚大な被害

2017 Triton

- 「Tri… マルウェアに感染
- 中東(… …
  (SIS… …

2017 NorPetya

- 「NorPetya…ランサムウェアが世界中で拡散
- 米メルク／… …製薬などで
  甚大な被害

2018

- 北米電力信頼度協議会(NERC)
- 基幹系統を危険な状態に…
- 電力企業に対し…

11億円の罰金

2018

- …
- …
- 製造システムが3日間停止

3日間のシステム停止
190億円の損害

20…

- …業務に影響

生産停止
1週間で4000万ドル

サイバー攻撃の脅威レベルが向上

半導体受託生産の世界大手 TSMC ランサムウェア感染 2018年8月

事象

- 作業ミス
- 工場ネットワーク

経過

Windows7端末

結果

- 3日間 の生産停止
- 190億円 の損害

レガシーOSの脆弱性

サイバー攻撃の脅威レベルが向上

市立病院 ランサムウェア被害 2018年10月

事象

- インターネット未接続のシステムに感染
- 感染経緯については不明

結果

- サーバには、約3,800人の診療記録が保存
- システムが使用できず、約1,100人分のデータが閲覧できなくなった

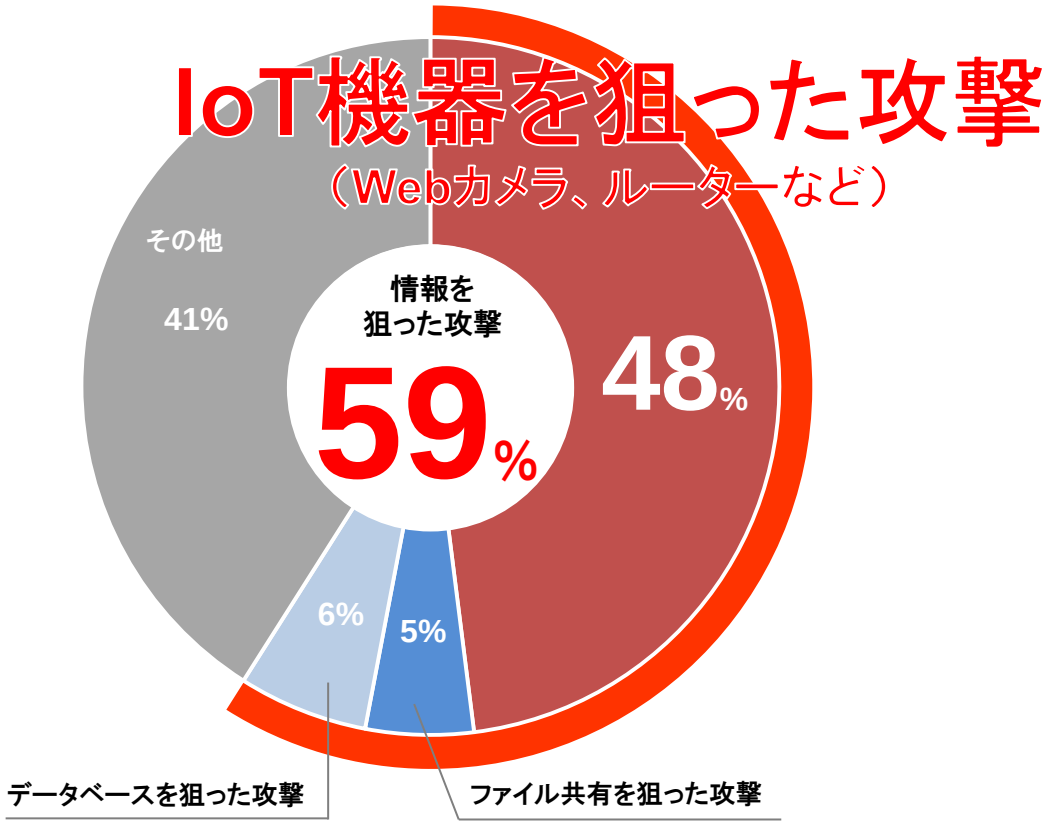
情報漏洩の危機

サイバーリスクが増大

1年間で観測されたサイバー攻撃件数

NICTER観測レポート2018

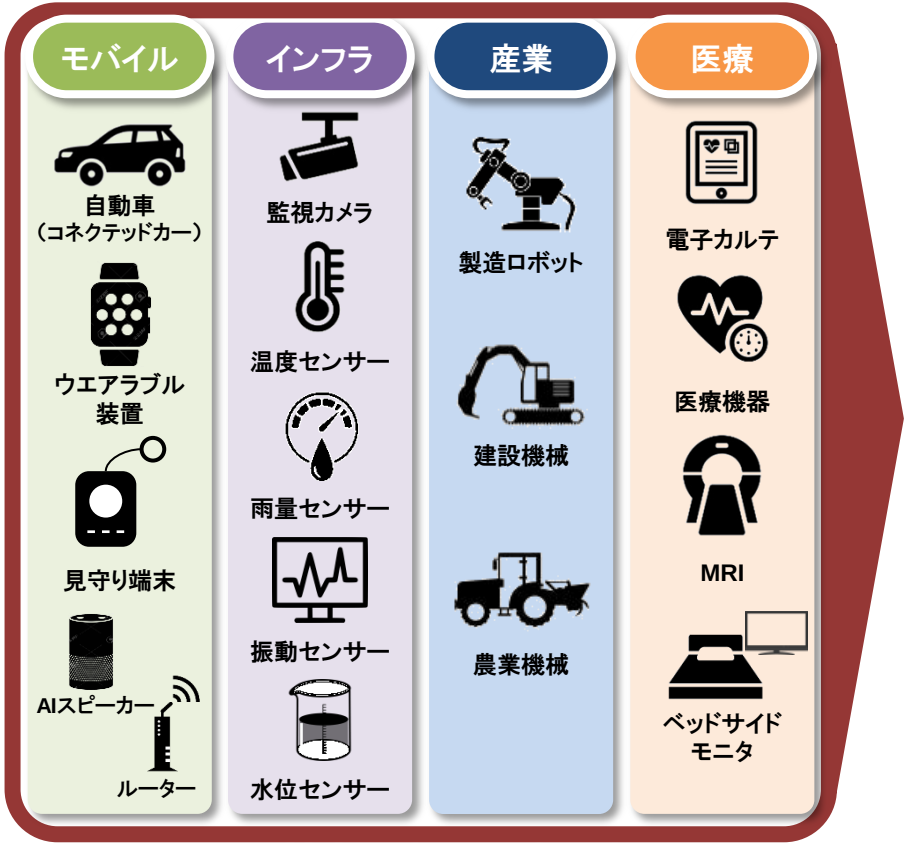
サイバー攻撃の内訳



03

被害が拡大する理由

大量の機器が感染

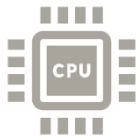


大型の **製造ロボット** や **自動車**
医療現場の **超小型センサー**

IoT機器特有の問題点

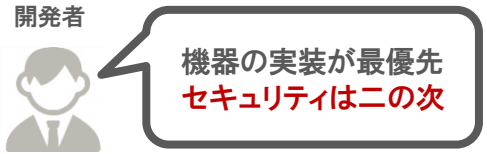
① リソースの貧弱さ

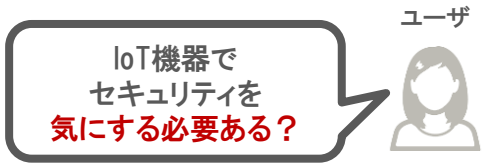
処理能力が小さい



ディスプレイなどの
表示装置がない

② セキュリティ意識の欠如





その結果・・・・

ウィルス対策
ソフトを使えない

最新の状態に
アップデート
出来ない

セキュリティの基本対策が取れない

取り巻く環境の変化

工場／医療現場 が 外部ネットワークへ接続

クローズドから 外部接続 へ

- IoTによる業務系接続増加
- 稼働データ活用／提示

制御システムの ITシステム化

- Windows／Linuxの汎用OS採用
- TCP/IPプロトコル採用

サイバー攻撃 の対象

- 制御関連セキュリティ事故増大
- 制御機器脆弱性発見数増大

標準化／規制化状況

- 認証制度（CSMS／EDSA）
- 標準化／ガイドライン整備

クローズド環境を前提、システムを停止できない事から

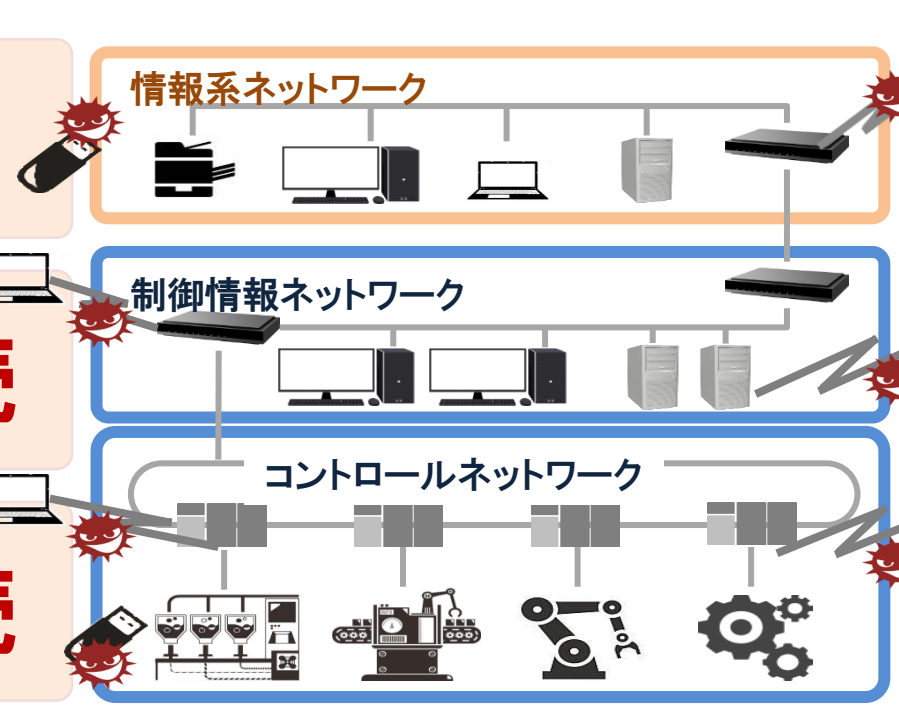
セキュリティ対策が未対応

被害リスクが増加

感染

外部接続

不正接続



侵入/攻撃

脆弱性

不正
アクセス

04

セキュリティ対策

重要なセキュリティ対策

サイバーセキュリティフレームワーク

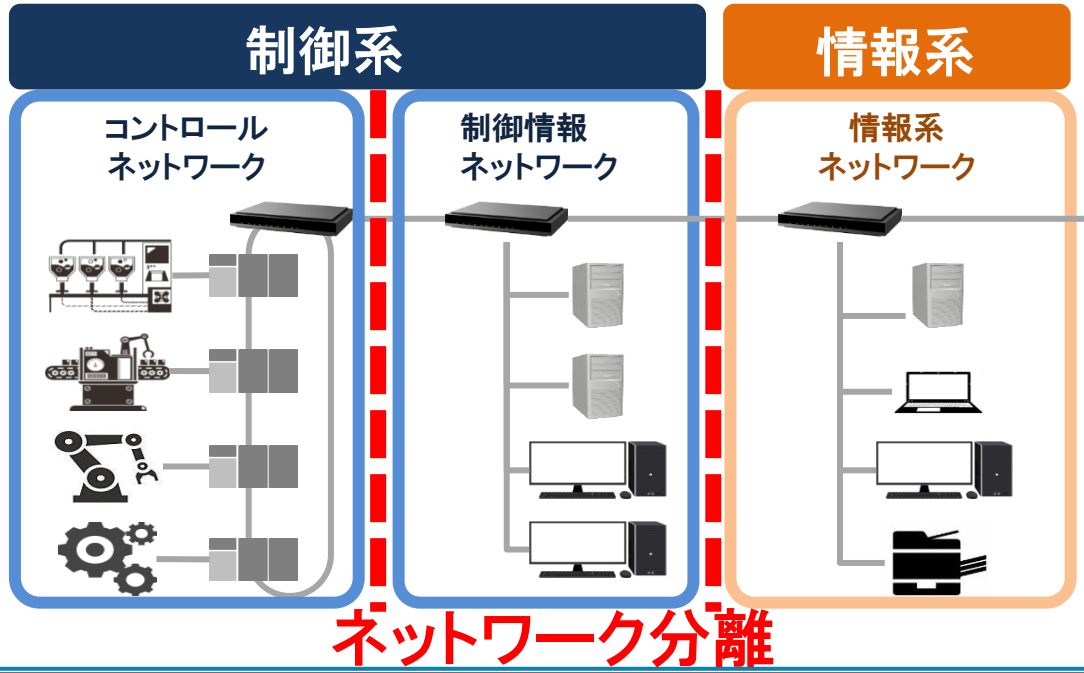
米国国立標準技術研究所(NIST)

攻撃から事前に守る
「特定と防御」が最も重要！

事前対策	特定	資産管理	ビジネス環境	ガバナンス
	防御	保護するための/手順	保守	保護技術
事後対策	検知	異常とイベント	継続的なモニタリング	検知プロセス
	対応	対応計画の作成	伝達	分析
		低減	改善	
	復旧	復旧計画の作成	改善	伝達

ネットワーク分離

セキュアレベルの異なるネットワークを分離して管理

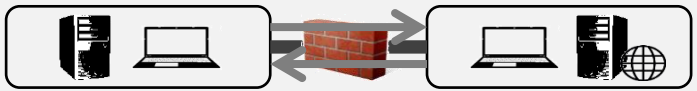
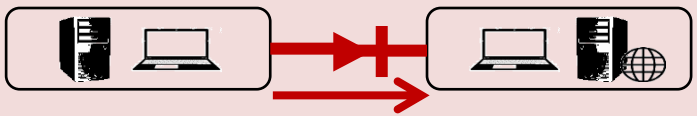


セキュリティ
レベルの違い

- ネットワークの違い
- アクセス可能な利用者
- セキュリティレベル

では、通信は？

片方向のみデータ通信する
データ・ダイオード

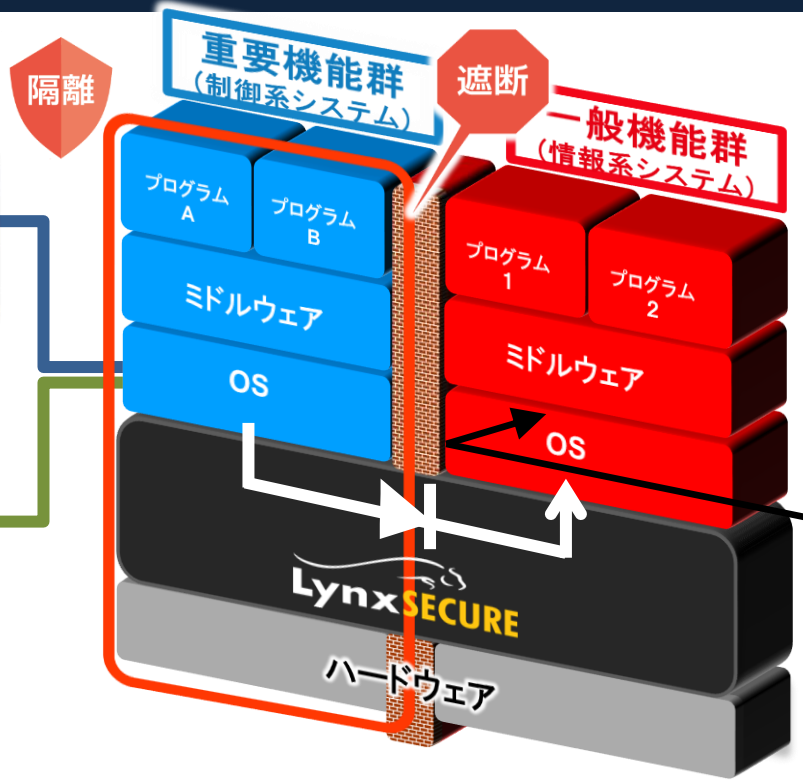
方式種別	概要	メリット／デメリット
通信無し	ネットワークが物理的に分離し通信手法を持たない 	データが必要な場合は、USB等のメディアや媒体を使用 **ウィルス感染のリスク**
TCP／IP通信	物理的な「接続」を構築した上で、ファイアウォール等でTCP/IPの論理的な通信制御を行う  TCP/IPによる双方向通信	双方向通信（TCP/IP）を制御 **脆弱性を突いたサイバー攻撃のリスク**
データ・ダイオード	物理的遠隔の上で、片方向だけデータ通信制御を行う  片方向通信のみ	LynxSECUREにて実現可能 LynxSECURE

05

のご紹介

LynxSECUREのコンセプト

隔離 ⊕ 遮断 ⊕ データ保護



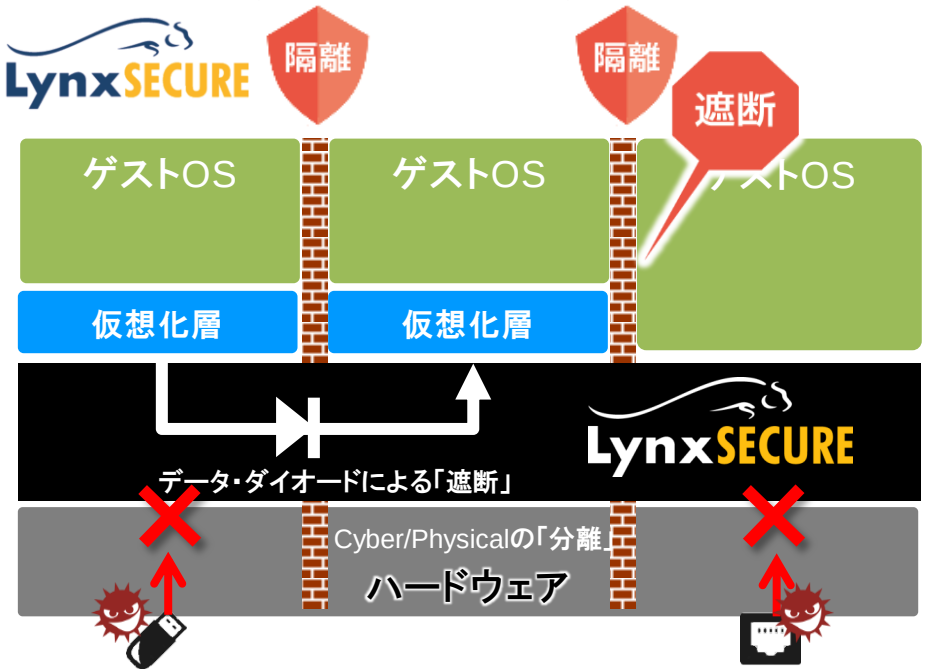
- 重要機能を **隔離**
- 被害の拡大を **遮断**
- **データ保護**

重要なセキュリティ対策

- ネットワーク分離
- データ・ダイオード方式

セキュリティの確保

ハードウェア(Physical空間)とソフトウェア(Cyber空間)の間に介在
不正なアクセスを完全にブロック！



06

LynxSECURE 適用事例のご紹介

セキュア レガシー

セキュア ログサーバー

オフィス

既存PCの利用継続可能
ネットワークを分離しレガシーOS延命を実現

サポート終了間近！

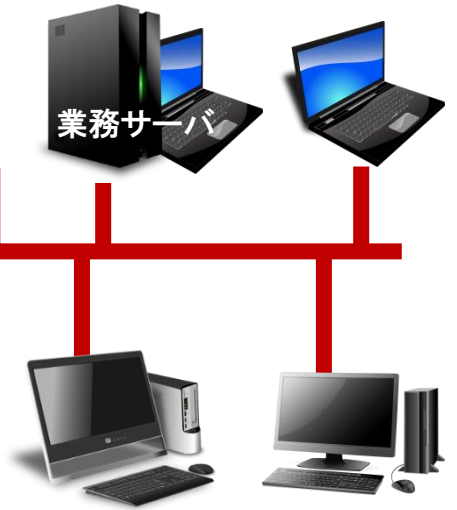
セキュア レガシー

レガシーシステム

LynxSECURE

社内LAN

社内LANに接続可能に！



費用も **低コスト！**

導入も **簡単！**

運用も **手間なし！**

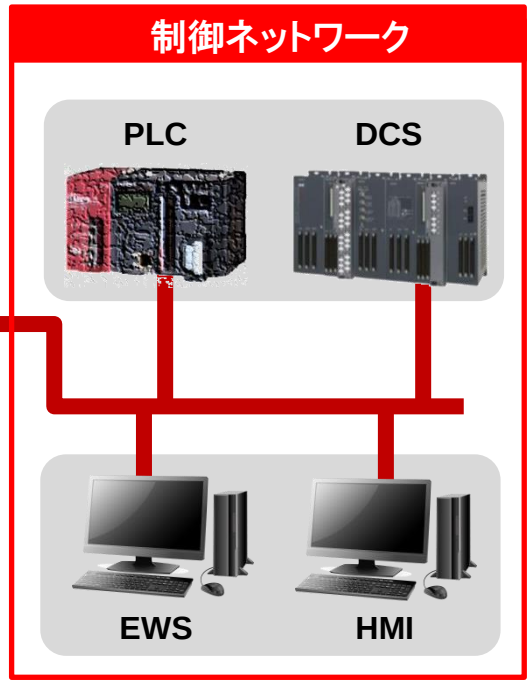
製造業

産業機器のレガシーOSの延命をしつつ制御システムへ接続！

機器とネットワークの
完全分離

セキュア レガシー

LynxSECURE



つながっていない産業機器を制御ネットワークへ接続！

産業機器の **安全** と **生産効率向上** を実現

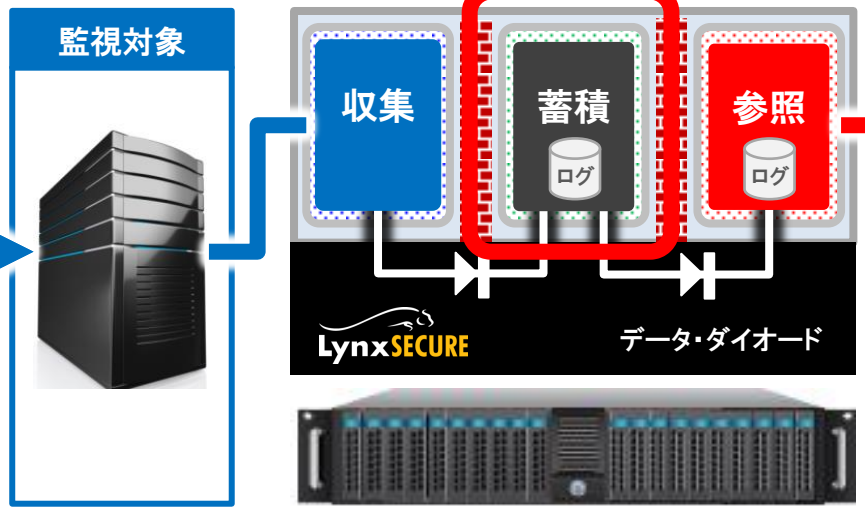
医療

重要なログを安心・安全に保護！
改ざん防止・ログ活用を両立！

VALUE HR

ISMS対応

セキュア ログサーバー



システムの **重要なログ** を **完全保護！**

製造業

工場内の重要データを有効活用！
遠隔地による状況監視・データ保護を実現！

不正発生時の追跡可能！

工場

フィールドネットワーク

コントロールネットワーク

HMI

PLC

- 生産実績
- 稼働状況
- 異常情報　など

セキュアログサーバー

収集

蓄積

ログ

参照

ログ

LynxSECURE

データ・ダイオード

監視・分析

重要データは企業の重要資産！隔離と遮断で完全保護！

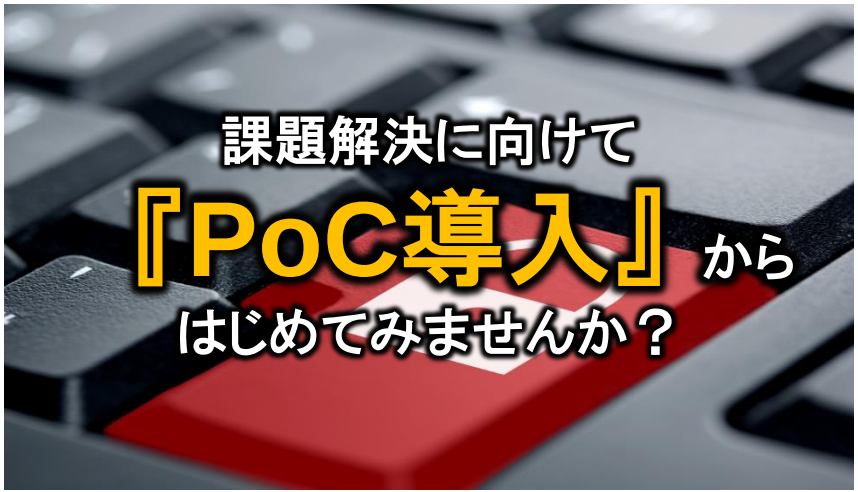
『LynxSECURE』お試し環境を提供！

LynxSECURE 評価キット

触ってみることでさまざまな新しいアイデアが生まれる！

LynxSECURE 機能
お手軽にPoC実施

ソフトウエア・
データダイオード
を使ったアプリケーション開発環境



※あくまで評価するための環境です。実際の導入にはご利用頂けません。

隔離 + 遮断 + データ保護

がお守りします

IoT機器をサイバー攻撃から守ります