# 工場セキュリティガイドライン
# 作成状況共有/説明資料

2022年1月6日

Edgecrossコンソーシアム - GUTP 合同
工場セキュリティWG

# 目次

- 工場セキュリティWG 活動の背景と目的
- 工場セキュリティWG 活動内容と成果物

# 工場セキュリティWG
# 活動の背景と目的

# 工場FA/OTシステムにかかわるセキュリティ事故/リスクが増大

- 工場で**生産停止/設備被害**につながる、**制御システムを狙ったサイバー攻撃**が増大

| | 自動車メーカ | 半導体メーカ | 製鉄所 |
|---|---|---|---|
| 被害 | 複数工場の生産停止<br>(被害総額 約1,400万ドル) | 複数工場の生産停止<br>(四半期売上高の約3%) | 生産設備の損傷 |
| 原因 | Zotobウイルス | WannaCryウイルス亜種 | トロイの木馬 |
| 感染経路 | 持込PC or NW | ウイルスチェック未実施<br>端末のNW接続 | 電子メールの<br>添付ファイル |

工場FA/OTシステムにかかわるセキュリティ事故の事例

# サプライチェーンリスクも増大

| 順位 | 「組織」向け脅威 |
|---|---|
| 1 | ランサムウェアによる被害 |
| 2 | 標的型攻撃による機密情報の窃取 |
| 3 | テレワーク等の<br>ニューノーマルな働き方を狙った攻撃 |
| 4 | サプライチェーンの弱点を悪用した攻撃 |
| 5 | ビジネスメール詐欺による金銭被害 |
| 6 | 内部不正による情報漏えい |
| 7 | 予期せぬIT基盤の障害に伴う業務停止 |
| 8 | インターネット上のサービスへの不正ログイン |
| 9 | 不注意による情報漏えい等の被害 |
| 10 | 脆弱性対策情報の公開に伴う悪用増加 |

出典：IPA「情報セキュリティ10大脅威 2021」

## 複雑なサプライチェーンによる脅威の例①：ランサムウェア"WannaCry"の猛威

参考：産業サイバーセキュリティ研究会第1回にて配布

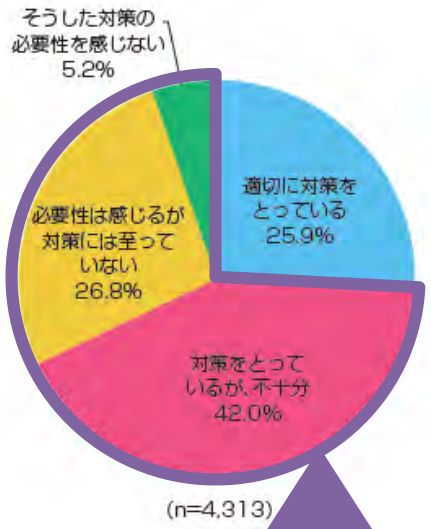
- 平成29年５月、世界の少なくとも約150か国において、Windowsの脆弱性を悪用したランサムウェア「WannaCry」に感染する事案が発生。
- **感染した欧州企業から、サプライチェーン経由で国内企業も感染。**


出典：経済産業省　産業サイバーセキュリティ研究会資料

# 製造業/工場におけるセキュリティ対策の状況

- 工場の**セキュリティ対策は不足**しており、**課題を抱え進んでいない**状況

図 135-4　セキュリティ対策の状況




資料：経済産業省調べ（2017年12月）

**74%が不足**

図 135-18　ものづくり企業におけるサイバーセキュリティ対策の方向性

**課題点①：中小企業を中心にサイバーセキュリティの必要性を感じていない**　危機意識喚起
（例）不安を感じないと回答した中小企業のうち６割「自社がターゲットになるとは思えない」
⇒対策の方向性：リスク認識の向上
具体策：（１）サイバーセキュリティリスク評価指標・ツール　（２）セミナー開催等

必要性は理解したが・・

**課題点②：何をしたらいいかがわからない**　対策方針指南
（例）ｻｲﾊﾞｰｾｷｭﾘﾃｨ上対策の障害:「何をしたらいいかがわからない」が中小企業で14%
⇒対策：対策として必要な考え方・手段を周知
具体策：（３）サイバーセキュリティ経営ガイドライン・中小企業の情報セキュリティ対策ガイドライン（IPA）
（４）サイバー・フィジカル・セキュリティ対策フレームワーク、（５）ベストプラクティス集の作成
（６）自己宣言制度（Security Action）（７）情報セキュリティ安心相談窓口等の設置（IPA等）

対策法が把握できたが・・

**課題点③：担い手となる人材がいない**　"人"
（例）対策の障害:「人材がいない」が中小企業で43%
⇒対策：★自社内で対策を講じる人材育成
☆専門業者への委託

**課題点④：コストがかかり投資が困難**　"金"
（例）対策の障害:「投資が困難」が大企業で52%
⇒対策：ソフトウェアや設備導入の際のコスト緩和
具体策：（８）コネクテッド・インダストリーズ税制

★（９）産業サイバーセキュリティセンターでの人材育成（IPA）
★☆（10）情報セキュリティスペシャリストの活用
☆（11）セキュアなベンダー・ツールの見える化（中企庁）
☆（12）セキュリティサービス審査登録制度

対策を講じたが・・

**課題⑤：対策が十分かがわからない、実際に攻撃を受けたらどうしたらいいのかわからない**　対策レビュー
（例）これまでのｻｲﾊﾞｰ攻撃による被害は全体で1割（大企業では1/4）
⇒対策：対策度合いの客観的評価が可能な仕組み、攻撃を受けた際の相談先・ガイドラインに則った対応策
具体策：（１）、（６）

資料：経済産業省作成

**必要？**

**必要な対策は何？**

**対策を実施する人は？金は？**

**実施済みの対策で十分？**

出典：経済産業省「2018年版ものづくり白書」

# 製造業/工場におけるセキュリティ対策の促進を目指して

- 工場FA/OTシステムのセキュリティ対策を前進させるためには、
  **①必要性や危機意識の啓発、**
  **②対策方法の解説、**
  **③アウトソースという選択肢の提示**

などが必要と認識

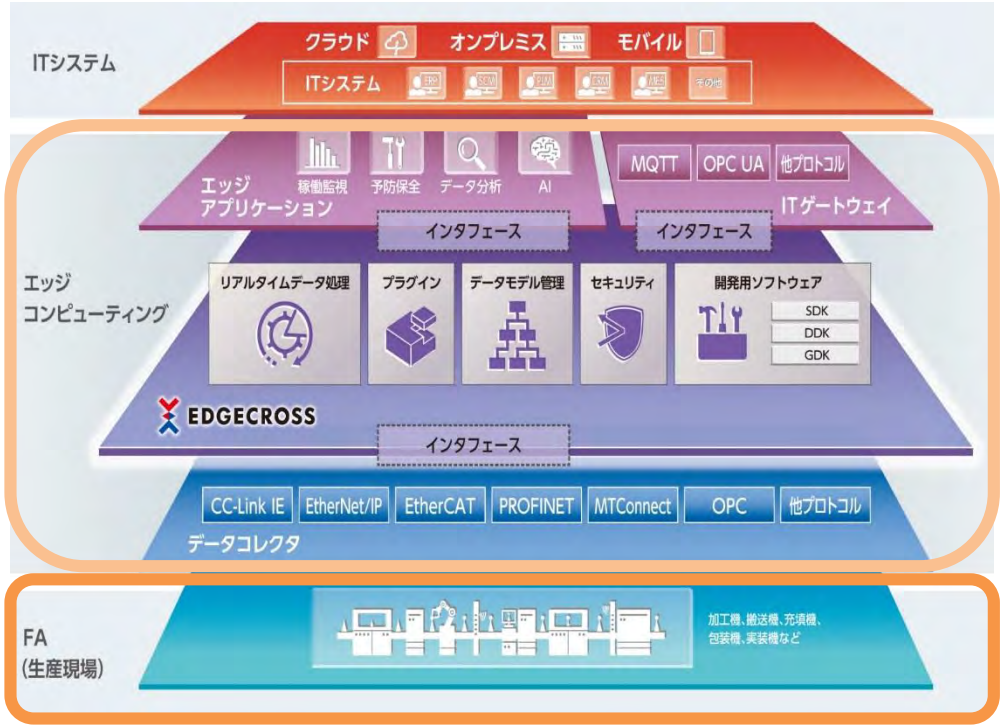
**⇒ 工場セキュリティガイドラインの作成・発信を推進**

# 工場セキュリティWG ガイドライン作成の取組み

**経済産業省**
**産業サイバーセキュリティ研究会**
**WG1 (制度・技術・標準化)**

- **ビルSWG** 座長：東大　江崎教授
  - ビルシステムにおける サイバー・フィジカル・セキュリティ対策 ガイドライン
- **電力SWG**
- **防衛産業SWG**
- **自動車産業SWG**
- **スマートホームSWG**
- **宇宙産業SWG**

工場のサイバー・フィジカル・システム
(Edgecrossの利用例)




**東京大学**
**グリーンICTプロジェクト**
**(GUTP)**
代表：東大　江崎教授

合同WG

**Edgecross コンソーシアム**
**セキュリティ**
**ガイドライン策定WG**
リーダ：NEC　桑田

**Edgecrossの**
**セキュリティ**

対象拡張

**FA/OTシステムの**
**セキュリティ**

**工場セキュリティWG**
**ガイドライン作成**

# 工場セキュリティWG
# 活動内容と成果物

# Edgecross – GUTP 合同　工場セキュリティWG　活動概況

WGの目的

**工場全体(制御/フィールドNWを含む)**のセキュリティ対策を啓発/促進する
ガイドライン作成及び情報発信

成果物

①工場向けセキュリティ対策ガイドライン　**概要編**　**作成中 (2022年2月発行予定)**
②工場向けセキュリティ対策ガイドライン　詳細編　作成中・一時中断 (概要編を優先、2022年発行予定)

WGリーダ

日本電気株式会社　サイバーセキュリティ事業部　桑田 雅彦

参画メンバー一覧（順不同、敬称略）

| 会社名 |
| --- |
| 三菱電機株式会社 |
| 日本電気株式会社 |
| 株式会社日立製作所 |
| オムロン株式会社 |
| PFU株式会社 |
| トレンドマイクロ株式会社 |
| CCDS（日立チャネルソリューションズ） |
| GUTP（東京大学、シムックスイニシアチブ、竹中工務店、GUTPコンサルティング）、ファナック、Fortinet |
| Edgecrossコンソーシアム事務局 |

**自ら工場をもち、
ガイドラインを利用する立場の
製造業企業も参加し共同作成**

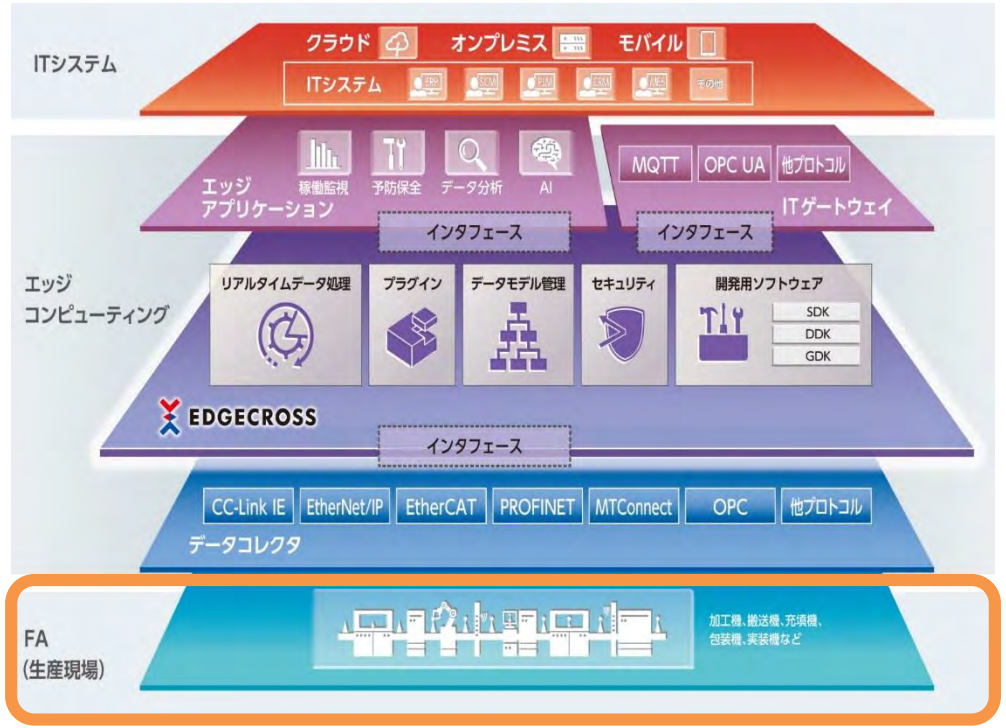
# 工場セキュリティガイドラインの想定読者

- 工場FA/OTシステム及びセキュリティの**調達要件を作成する人**
  - 調達対象機器/装置に対する要件を含む
- FA/OTシステム**利用者**(生産技術部門、生産管理部門、工作部門など)、及び**経営層**(投資承認者)
- 同、システム**構築者**、**管理者**、**運用者**、**保守者**
- 同、**機器/装置メーカ**

# 工場セキュリティガイドラインの対象範囲

- **工場FA/OTシステム(新設/既存)**のセキュリティ対策要件ガイドライン
- **FA/OTシステムに特有の部分に焦点**を当てる
- 第１版は、概要編として、**必要最小限の基本要件**に絞った内容を提示予定

工場のサイバー・フィジカル・システム (Edgecrossの利用例)




**対象範囲**

**FA/OTシステムの**
**セキュリティ**

# 工場セキュリティガイドラインの目的、位置付け

- **①必要性や危機意識の啓発、②対策方法の解説、 ←工場の価値観/用語を正**
  **③アウトソースという選択肢の提示**

- 工場FA/OTシステム及びセキュリティの**調達要件モデルを提示**
  - 調達対象機器/装置に対する要件を含む
- **新設**システムだけを対象にするのではなく、
  **既存**システムのセキュリティ対策レベルを向上させるためには、どうすれば良いかを提示
- セキュリティ対策を適用できない既存の古い機器/装置から、
  **新しい機器/装置へ置き換える動機づけ**になる内容
- ただし、**古い機器/装置を継続利用せざるをえない場合**に、
  どのように対処すれば良いかを提示

- 既存の一般的なガイドラインの内容を参照/流用しながら、
  **FA/OTシステムに特有の部分に焦点**を当てた内容を提示

# [成果物] 工場セキュリティガイドライン 概要編 目次(予定)

1．はじめに
- 1.1 背景、目的
- 1.2 想定読者
- 1.3 対象範囲、位置付け
- 1.4 全体構成、概要
- 1.5 基本的な方針/考え方 [BC/SQDCの観点]
- 1.6 用語/略語
- 1.7 関連/参考資料

2．工場FAシステムのセキュリティ対策の考え方
- 2.1 セキュリティ対策の目的・機能
- 2.2 セキュリティ対策検討・企画に必要な要素
- 2.3 セキュリティ対策検討・企画の考え方

3．対象とするFAシステムの全体像/基本構成
- 3.1 想定企業
- 3.2 想定組織構成
- 3.3 想定生産ライン
- 3.4 想定業務
- 3.5 想定データ
- 3.6 ゾーンの定義

4．対象FAシステムのセキュリティ保護対象と脅威・影響
- 4.1 想定保護対象
- 4.2 想定される脅威・影響

5．FAシステムを取り巻く社会的セキュリティ要件
- 5.1 法規制、標準規格、ガイドライン準拠にかかわる要件
- 5.2 国・自治体からの要求
- 5.3 業界からの要求
- 5.4 市場・顧客からの要求
- 5.5 取引先からの要求
- 5.6 出資者からの要求

6．セキュリティ対策の全体像
- 6.1 セキュリティ対策企画・導入の進め方
- 6.2 多面的なセキュリティ対策の全体像
  (物理面、システム構成面[ネットワーク面、装置面]、
  運用・管理面[OODA]、維持・改善面[PDCA]、サプライチェーン面)
- 6.3 スマート工場の実現に向けた段階的な実現レベル向上
- 6.4 FAシステム及び機器の提供ベンダ／メーカへの対策要求
- 6.5 セキュリティベンダが提供するサービス／製品の活用

7．中小企業の工場におけるセキュリティ対策の考え方

8．参考

9．付録
- 9.1 チェックリスト
- 9.2 調達仕様書テンプレート(記載例)

別冊．取り組み事例
1. Edgecross/IoTゲートウェイのセキュリティ対策
2. 三菱電機/FAシステムのセキュリティ対策
3. オムロン/コントローラのセキュリティ対策

# 工場セキュリティガイドライン 概要編(作成中) の骨子 (1/4)

- 2章にて、まず、**工場FAシステムのセキュリティ対策をどのように考えれば良いのか**、
  その**考え方や論理全体の流れを先に把握してもらう位置付け**で、

  **製造業/工場が重視する価値軸：BC/SQDCなどの視点と対応づけ**ながら、
  **セキュリティ対策の目的・機能**を示し、
  3～5章で提示する、**対策検討・企画に必要な要素**が何か、及び
  **要素に基づき対策を考え出す方法(論理)**を説明

# 工場セキュリティガイドライン 概要編(作成中) の骨子 (2/4)

- 3章にて、**典型的な工場FAシステムのユースケース**を設定し、
  4章にて、**保護対象**、**想定脅威**、**リスク/影響度**を整理
- 製造業/工場の事業/業務にとって**重要な価値軸：BC/SQDC**に対して、
  セキュリティリスクがどのような影響を及ぼすのかを結びつけ、
  **リスク対応の優先度**を整理

- 5章にて、**法規制・標準規格・ガイドライン準拠**や**各種ステークホルダからの要求**
  といった、**環境要件(社会的セキュリティ要件)**を整理

# 工場セキュリティガイドライン 概要編(作成中) の骨子 (3/4)

- 6章にて、システム構成面の**技術的防御策**(物理、NW、FA機器/装置)、**運用・管理面**(OODA)、**維持・改善面**(PDCA)、**サプライチェーン面**に分け、FAシステムの**ライフサイクル全体にわたる対策**の概要を整理
- **必要最小限の基本的な対策**から始め、FAシステムのDX化に応じて**段階的にレベルを向上**させていく進め方を提示
- 工場だけで対策を実現するのが困難な場合は、**FAシステム及び機器の提供ベンダやメーカへ対策を要求**したり、**セキュリティベンダが提供するサービス／製品を活用**すれば良いことを**紹介**

- 7章にて、**中小企業の工場**におけるセキュリティ対策の考え方にかかわる補足を提示

# 工場セキュリティガイドライン 概要編(作成中) の骨子 (4/4)

- 付録として、
  ガイドラインの内容に基づく**チェックシート**、及び
  **調達仕様書テンプレート(記載例)**を提供
- 別冊として、**取り組み事例**を提示


https://www.edgecross.org/