経済産業省

産業分野におけるサイバーセキュリティ政策について

経済産業省　商務情報政策局

サイバーセキュリティ課

１．サイバー攻撃の現状

２．経済産業省のサイバーセキュリティ政策の全体像

３．サイバー・フィジカル・セキュリティ対策フレームワーク

４．工場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
ガイドラインの概要および普及啓発

５．工場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
ガイドライン拡充版の検討

サイバー攻撃の現状

- 企業等の情報を暗号化して金銭をゆすり取る「ランサムウェア攻撃」や国家支援型の攻撃集団等が特定の企業を執拗に狙う「標的型攻撃」が引き続き多く見られる。
- 特に、セキュリティ対策に弱点のある取引先等が攻撃経路として狙われ、被害が拡大する「サプライチェーンの弱点を悪用した攻撃」により、甚大な影響が生じている。

情報セキュリティ10大脅威 2023

順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5位	テレワーク等のニューノーマルな働き方を狙った攻撃
6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策情報の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害
10位	犯罪のビジネス化（アンダーグラウンドサービス）

<出典：(独)情報処理推進機構(IPA)、2023.1.25>

事例

- 2022年10月末、**国内の公立病院がランサムウェア攻撃を受け、電子カルテシステムに障害が発生**し、**緊急以外の手術や外来診療が一時停止する等**通常診療ができない状況に。
- **病院の給食を委託していた業者のサーバーからウイルスが侵入**した可能性が高いとみられている。
- ２ヶ月超にわたり通常診療を見合わせ。

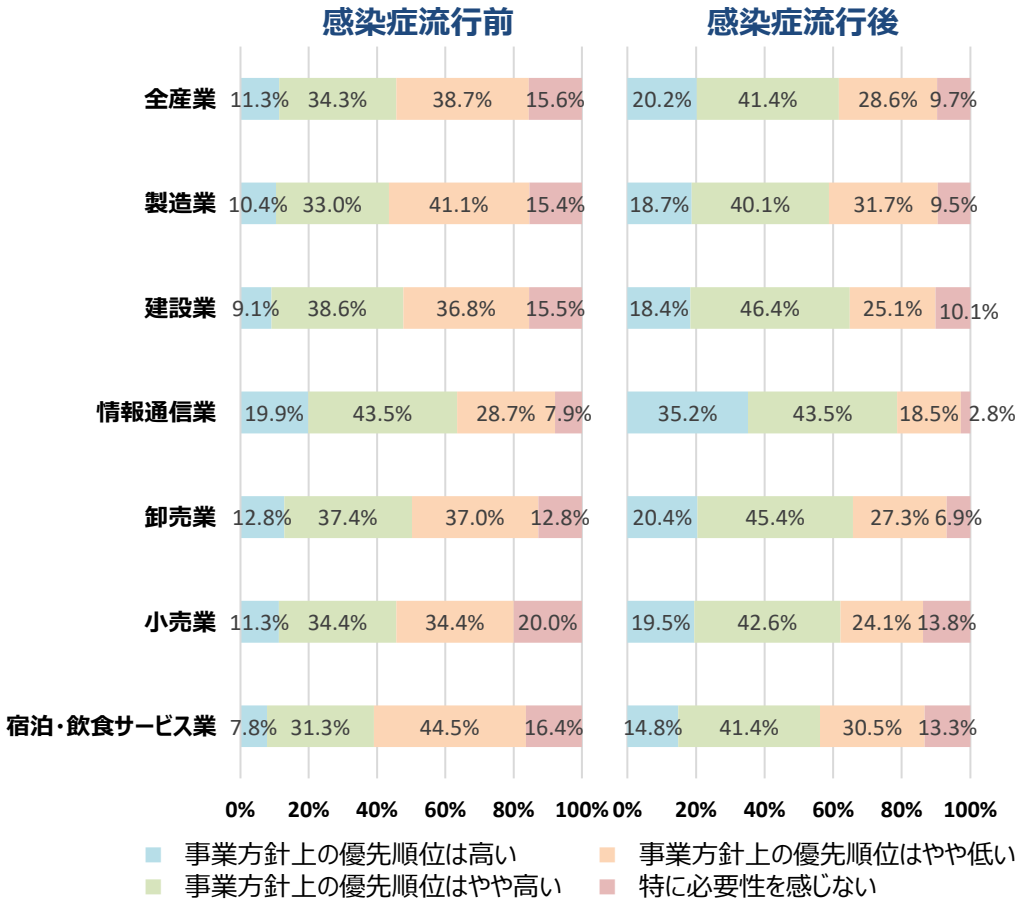
- 2022年11月、警察庁とNISCが日本国内の学術関係者、シンクタンク研究員等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラム(マルウェア)を実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されていると注意喚起。

- ランサムウエアグループ「Hive（ハイブ）」は、機器の脆弱性やメールを通じて被害者のネットワークに侵入。2021年6月以来、ハイブは、世界中で1,500以上の組織を標的とし、1億ドルを超える身代金を獲得していた。
- 2023年1月、米連邦捜査局（FBI）等の米当局が、1年半をかけてランサムウエアグループに対する破壊作戦を実施したと発表。

デジタル化の進展とサイバーセキュリティ対策の必要性

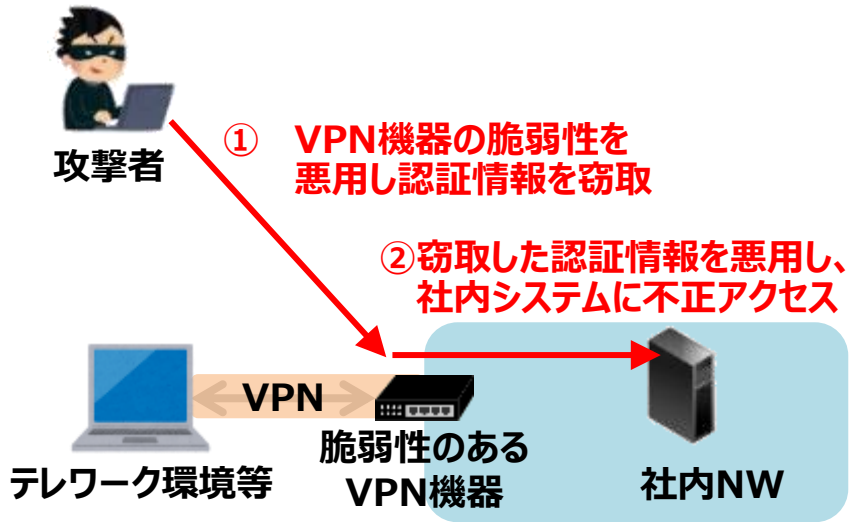
- デジタル化に対する意識は、コロナ禍の前後で、**産業領域を問わず大きく変化**。
- 一方、テレワークの利用等が増える中、VPNの脆弱性を突いたサイバー攻撃が増加するなど、**サイバー攻撃の脅威はあらゆる産業において無縁ではなくなっている**。

デジタル化に対する優先度の変化



（出典）中小企業庁「中小企業白書2021」

VPN機器に対する不正アクセス



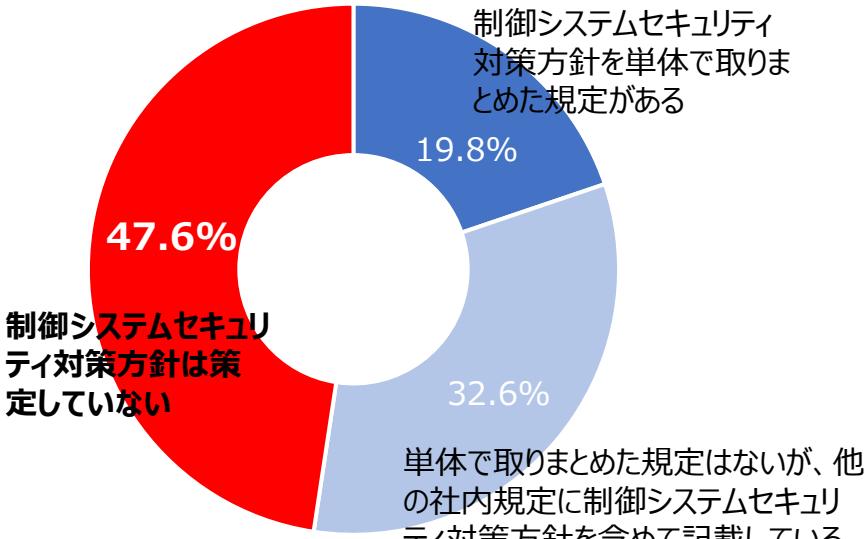
事例：Fortinet製FortiOSの脆弱性

2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等その後追加公開があり、対象が計8.7万台に拡大。

セキュリティ対策の遅れ

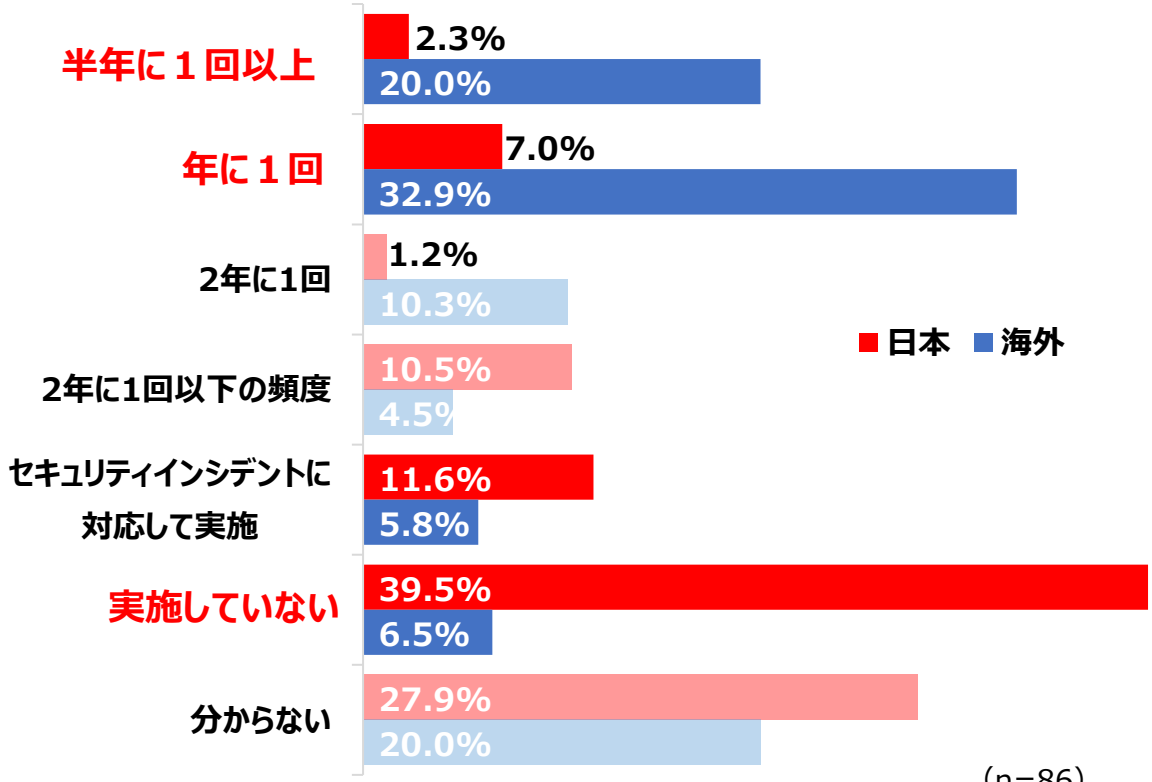
- アンケート調査によると、**制御系セキュリティシステムの対応方針を策定していない企業が５割**存在。
- セキュリティアセスメントについては、**実施していないと回答する企業が４割存在**し、５割以上が半年又は年に１回以上実施する海外と大きく乖離。

制御システムセキュリティ対策方針の整備状況



（n=86）

制御システムに対するセキュリティアセスメントの実施状況



（n=86）

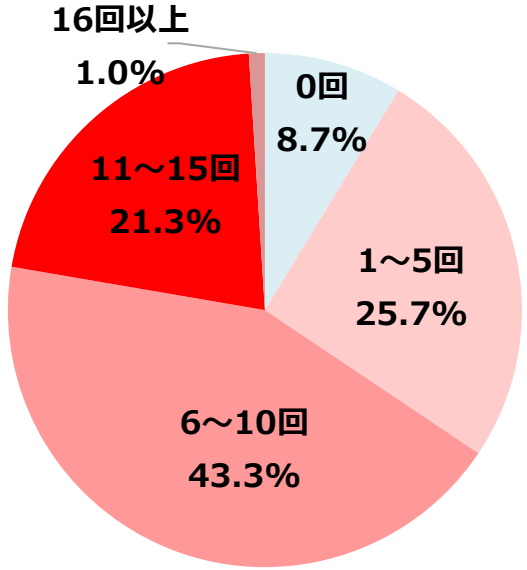
出典：KPMGサイバーセキュリティサーベイ2022
https://assets.kpmg/content/dam/kpmg/jp/pdf/2022/jp-cyber-security-survey2022.pdf

制御系システムへのサイバー攻撃の影響

- 制御系システムを有する国内の製造・電力・石油/ガス産業へのアンケート調査によると、直近１年で、**サイバー攻撃によりシステムの1日以上のシステムの中断を９割の組織が経験**。
- そのうち**２日以上システムの中断が続いたと回答した組織は８割**であり、絶えず稼働することが前提のシステムの中断は、短期間の中断でも組織の収益に大きく影響。**金銭的損害は平均で2.7億円**。

システムの中断を経験した回数

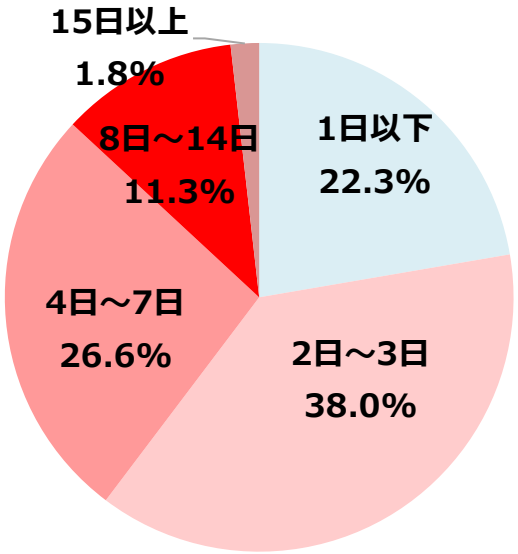
質問：「過去 12 か月間に、サイバー攻撃 （マルウェアの感染、脆弱性を悪用する攻撃、不正アクセスなど）により、あなたの組織の ICS/OT システムの運用は何回中断しましたか」



（n=300）

システムが中断した期間

質問：過去 12 か月間の間、サイバー攻撃の結果、組織の ICS/OT システムの運用は通常、どのくらいの期間中断しましたか」



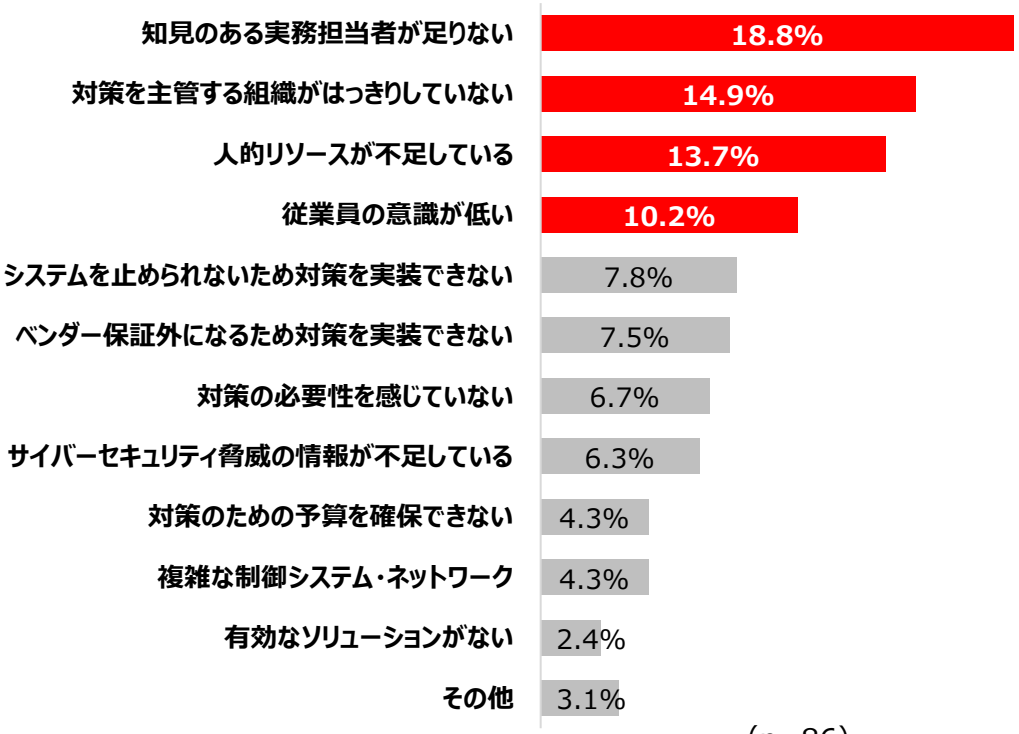
（n=274）

出典：2022年 トレンドマイクロ株式会社 産業制御システムのサイバーセキュリティ実態調査を基に経済産業省が作成
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220711-01.html

制御システムのセキュリティ人材の不足

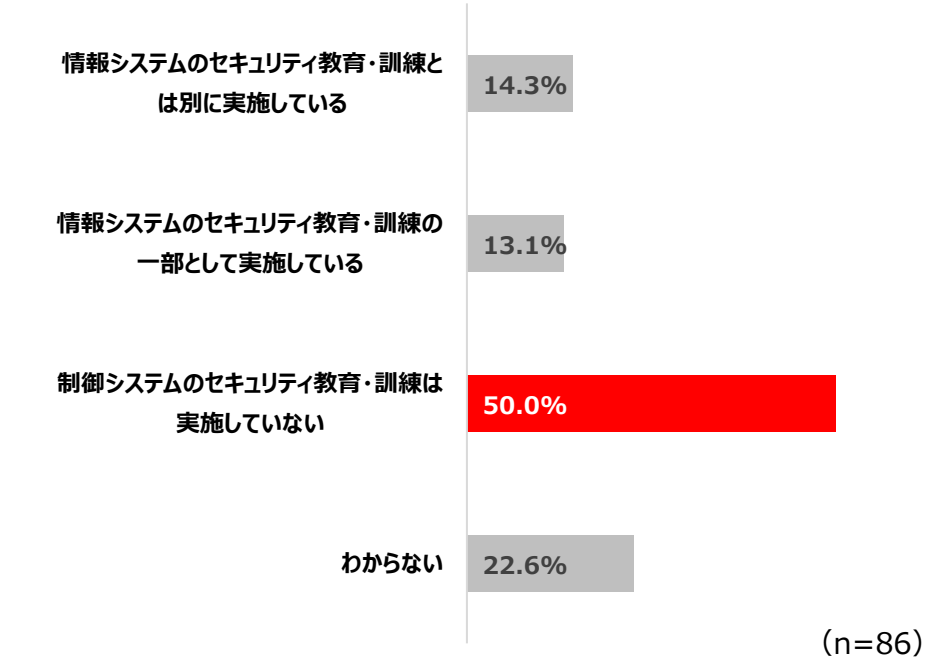
- 制御システムの対策が進んでいない原因として、知見・人的リソースの不足、主管組織が明確になっていないことが主な原因として挙げられており、**組織のセキュリティの中核を担う人材がいない**。
- 制御システムの**「セキュリティ教育・訓練を実施していない」と回答する企業が５割**に上っており、制御システムのセキュリティ人材の確保・育成は大きな課題。
- 制御システムのセキュリティ対策方針を主体的に検討し、実際のアセスメントを実施できる、経営層と現場担当者を繋ぐ**中核人材の育成が不可欠**。

制御システムセキュリティ対策が進んでいない原因



（n=86）

制御システムのセキュリティ教育・訓練の実施状況



（n=86）

出典：KPMG サイバーセキュリティサーベイ2022
https://assets.kpmg/content/dam/kpmg/jp/pdf/2022/jp-cyber-security-survey2022.pdf

１．サイバー攻撃の現状

２．経済産業省のサイバーセキュリティ政策の全体像

３．サイバー・フィジカル・セキュリティ対策フレームワーク

４．工場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
ガイドラインの概要および普及啓発

５．工場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
ガイドライン拡充版の検討

サイバーセキュリティ政策の推進体制

内 閣　内閣総理大臣

国家安全保障会議（NSC）

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）※

本部長　内閣官房長官

副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣

閣僚本部員
- 国家公安委員会委員長
- デジタル大臣
- 総務大臣
- 外務大臣
- 経済産業大臣
- 防衛大臣
- 経済安全保障担当大臣

有識者本部員

上沼 紫野	弁護士（虎ノ門南法律事務所）
遠藤 信博	日本電気(株)特別顧問
後藤 厚宏	情報セキュリティ大学院大学学長
酒井 啓亘	京都大学大学院法学研究科教授
桜井 敬子	学習院大学法学部教授
田中 孝司	KDDI(株)代表取締役会長
土屋 大洋	慶應義塾大学大学院教授
松原実穂子	日本電信電話(株)チーフ・サイバーセキュリティ・ストラテジスト
村井 純	慶應義塾大学教授

① サイバーセキュリティ戦略の案の作成及び同戦略の実施推進
② 国の行政機関・独法・指定法人における対策基準の作成／監査等
③ 国の行政機関・独法・指定法人で発生した重大事象について原因究明調査等
④ サイバーセキュリティに関する事象が発生した場合の国内外の関係者との連絡調整
⑤ 重要施策の企画・調査・審議、経費見積り方針等の指針の作成、総合調整

重要インフラ専門調査会 | 研究開発戦略専門調査会 | 普及啓発・人材育成専門調査会 | サイバーセキュリティ対策推進会議（CISO等連絡会議）

緊密連携

デジタル庁

デジタル社会の形成に向けた司令塔としてデジタル改革を推進

連携

サイバーセキュリティ協議会

官民の多様な主体が相互に連携した、より早期の段階での、サイバーセキュリティの確保に資する情報の迅速な共有等

<重要インフラ所管省庁>

〔所管重要インフラ事業におけるサイバーセキュリティの確保〕

- 金融庁（金融機関）
- 総務省（地方公共団体、情報通信）
- 厚生労働省（医療、水道）
- 経済産業省（電力、ガス、化学、クレジット、石油）
- 国土交通省（鉄道、航空、物流、空港）

<その他関係省庁>

文部科学省（セキュリティ教育）等

協力

（事務局）

内閣官房 内閣サイバーセキュリティセンター（NISC）（2015.1.9 内閣官房組織令により設置）

〔各省のサイバーセキュリティ施策の統一性保持のための総合調整〕

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）

副センター長（内閣審議官）

政府関係機関・情報セキュリティ横断監視・即応調整チーム（GSOC）

情報セキュリティ緊急支援チーム（CYMAT）

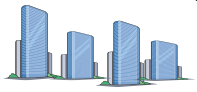
協力

閣僚本部員６省庁

〔各省の所掌に基づくサイバーセキュリティ施策の実施〕

- 警察庁（サイバー犯罪取締り）
- デジタル庁（デジタル社会形成）
- 総務省（通信・ネットワーク政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）


重要インフラ事業者等


政府機関（各府省庁）

企業


個人

産業サイバーセキュリティ研究会とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日　開催
第２回：平成30年　5月30日　開催
　アクションプラン（４つの柱）を提示
第３回：平成31年　4月19日　開催
　アクションプランを加速化する３つの指針を提示
第４回：令和2年　　4月17日　開催（電話開催）
　産業界へのメッセージを発信
第５回：令和2年　　6月30日　開催
　サイバーセキュリティ強化運動の展開
第６回：令和３年　　４月２日　開催
　アクションプランの持続的発展と、新たな課題へのチャレンジへ
第７回：令和４年　　4月11日　開催
　産業界へのメッセージを発信

構成員

- 泉澤　清次　三菱重工業株式会社取締役社長　※2022年4月開催時点
- 遠藤　信博　日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社取締役会長等
- 大林　剛郎　日本情報ｼｽﾃﾑ･ﾕｰｻﾞｰ協会会長、株式会社大林組代表取締役会長
- 櫻田　謙悟　経済同友会代表幹事、ＳＯＭＰＯホールディングスグループＣＥＯ取締役　代表執行役社長
- 篠原　弘道　日本電信電話株式会社取締役会長
- 東原　敏昭　株式会社日立製作所取締役会長　代表執行役
- 船橋　洋一　一般財団法人アジア・パシフィック・イニシアティブ理事長
- 村井　純(座長)慶應義塾大学教授
- 渡辺　佳英　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

オブザーバー　NISC、警察庁、金融庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省、デジタル庁

WG１（制度・技術・標準化）

第１回　平成30年2月7日
第２回　平成30年3月29日
第３回　平成30年8月3日
第４回　平成30年12月25日
第５回　平成31年4月4日
第６回　令和2年3月（書面開催）
第７回　令和2年10月（書面開催）
第８回　令和3年３月15日
第９回　令和4年4月4日

１．サプライチェーン強化パッケージ

WG２（経営・人材・国際）

第１回　平成30年3月16日
第２回　平成30年5月22日
第３回　平成30年11月9日
第４回　平成31年3月29日
第５回　令和2年1月15日
第６回　令和2年8月25日
第７回　令和3年2月18日
第８回　令和4年3月23日
第９回　令和5年3月29日

２．経営強化パッケージ
３．人材育成・活躍促進パッケージ

WG３（サイバーセキュリティビジネス化）

第１回　平成30年4月4日
第２回　平成30年8月9日
第３回　平成31年1月28日
第４回　令和元年8月2日
第５回　令和2年3月(書面開催)
第６回　令和3年3月10日
第７回　令和4年4月6日

４．ビジネスエコシステム創造パッケージ

産業サイバーセキュリティの加速化指針

１．『グローバル』をリードする
２．『信頼の価値』を創出する~Proven in Japan~
３．『中小企業・地域』まで展開する

経済産業省におけるサイバーセキュリティ政策の全体像

- サイバー攻撃の高度化・多様化が生じている現状を認識しつつ、我が国**産業界へのサイバー攻撃を抑制・防御**し、事業活動への影響を最小化する。そのために国が行うべき政策を企画・実行する。
- その上で、サイバーセキュリティの確保に向けた各種の取組を、**我が国産業競争力の強化**につなげる。

①サプライチェーン全体での対策強化

- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の具体化・実装
- 経営ガイドラインの活用促進
- サイバーセキュリティお助け隊サービスの普及促進
- 重要インフラ等を守る高度セキュリティ人材の育成（中核人材育成プログラム）
- 日米欧によるインド太平洋地域向けの能力構築支援

サイバーセキュリティ お助け隊

IPA 産業サイバーセキュリティセンター
Industrial Cyber Security Center of Excellence（ICSCoE）

②国際連携を意識した認証・評価制度等の立上げ

- IoT適合性評価制度の検討、国際制度調和に向けた調整
- SBOM（Software Bill of Materials）の活用促進
- QUAD上級サイバー会合、G7等を通じた各国間連携

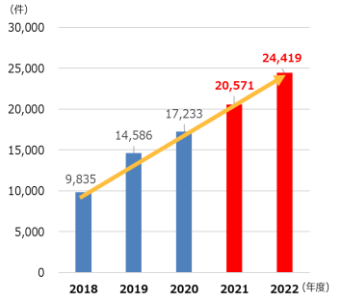
SBOMの概念的イメージ

ID	サプライヤー名	コンポーネント名	コンポーネントのバージョン	その他の一意の識別子	依存関係	SBOM作成者	タイムスタンプ
1	Company A	Application	1.1	234	Primary	Company A	05-09-2022 13:00:00
2	Company B	Browser	2.1	334	Included in #1	Company B	04-18-2022 15:00:00
3	Mr. C	Compression Engine	3.1	434	Included in #2	Company A	05-09-2022 13:00:00
4	Community P	Protocol	2.2	534	Included in #1	Company A	05-09-2022 13:00:00

③政府全体でのサイバーセキュリティ対応体制の強化

- 国境を越えて行われるサイバー攻撃へのJPCERT/CCの対処能力の向上
- 重要インフラ事業者等での事案発生時の初動支援を行うJ-CRATの体制強化
- 改正保安３法を踏まえた事故調査体制の構築
- サイバー攻撃被害情報の共有促進に向けた検討

サイバー攻撃事案の調整件数（年度集計）



④新たな攻撃を防ぎ、守るための研究開発の促進（サイバーセキュリティ産業新興）

- 先進的サイバー防御機能・分析能力の強化
- セキュリティ産業の成長加速化、製品/サービスの国内自給率向上に向けた政策検討

中小企業向けセキュリティ対策

● 中小企業の情報セキュリティ対策ガイドライン（第3.1版 2023年4月）

中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、を実践する際の手順や手法をまとめたもの。付録としてクラウドサービスの安全利用やセキュリティインシデント対応に関する手引きなどがある。

中小企業の情報セキュリティ対策ガイドライン

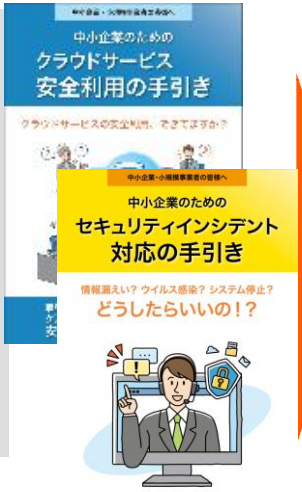
経営者向けの解説

経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説

企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

付録6、8:クラウドサービス安全利用の手引き、セキュリティインシデント対応手引き



【クラウドサービス導入時の考慮ポイントの例】

- ✓ 選択時のポイント（利用業務の明確化、取り扱う情報の重要度確認、クラウドサービスの安全・信頼性確認　等）
- ✓ 運用時のポイント（管理担当者、利用者範囲の決定　等）
- ✓ セキュリティ管理のポイント（利用者サポート体制の確認、利用終了時のデータ確保、適用法令や契約条件の確認　等）

【セキュリティインシデント対応時等の例】

- ✓ インシデント対応の基本ステップ（ステップ１ 検知・初動対応、ステップ２ 報告・公表、ステップ３ 復旧・再発防止）に関する具体例
- ✓ インシデント発生時の相談窓口・報告先　等

● 「SECURITY　ACTION」

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度。25万者を超える中小企業が宣言。

★一つ星

情報セキュリティ５か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

● サイバーセキュリティお助け隊サービス

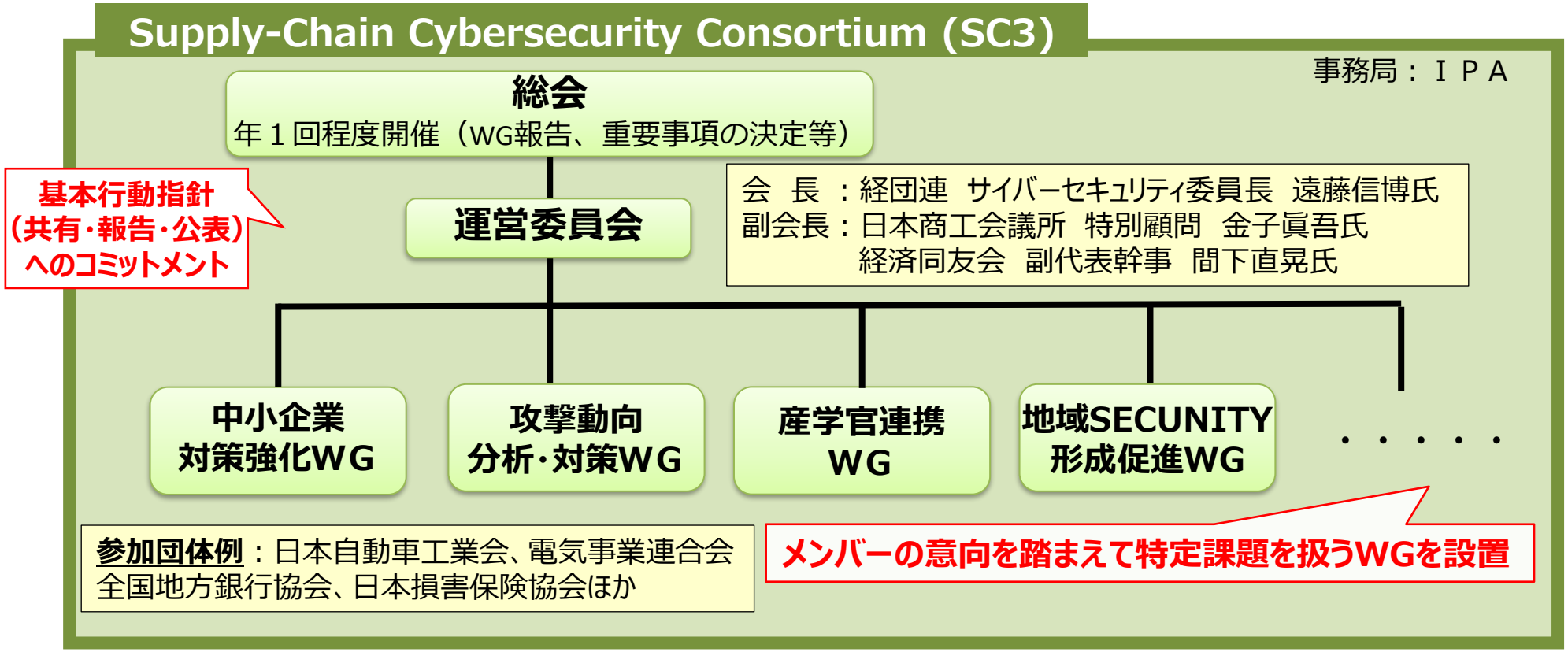
相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など各種サービス内容を要件としてまとめた基準を満たすワンパッケージサービス。
（2023年7月時点で35事業者）

サイバーセキュリティ お助け隊

IT導入補助金に
「セキュリティ推進枠」創設

サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）

- **趣　旨:** 大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ、「基本行動指針※」の実践と中小企業・地域を含めたサプライチェーンのサイバーセキュリティ対策を産業界全体の活動として展開していく。
  ※サイバー攻撃事案発生時における、「共有、報告、公表」によるリスクマネジメントの徹底。
- **参加者:** 経済団体、業種別業界団体　等（2023年６月末時点で177会員）
- **設立日:** 2020年11月1日（設立総会：2020年11月19日）
- **活　動:** 特定の課題についてWGを設置し、具体的アクションを展開。



【参考】コンソーシアムの構成員

- 経済三団体（経団連、日本商工会議所、経済同友会）から役員が出ているほか、幅広い業界　団体・個社が参加。（2023年６月末日時点、101団体含む177会員）

役員
- 会　長　：一般社団法人 日本経済団体連合会　副会長/サイバーセキュリティ委員長　遠藤信博氏
- 副会長：日本商工会議所　特別顧問　金子眞吾氏　、　公益社団法人経済同友会　副代表幹事　間下直晃氏

団体会員リスト

特定非営利活動法人 日本ネットワークセキュリティ協会
一般社団法人 ソフトウェア協会
一般社団法人 日本金型工業会
鋳型ロール会
一般社団法人 日本陸用内燃機関協会
一般社団法人 日本機械工業連合会
石油連盟
特定非営利活動法人 ITコーディネータ協会
一般社団法人 日本電子回路工業会
一般社団法人 全国地方銀行協会
一般社団法人 日本自動車工業会
日本商工会議所
一般社団法人 中小企業診断協会
一般財団法人 日本自動車査定協会
一般社団法人 日本鋳鍛鋼会
日本筆記具工業会
一般社団法人 日本ボディファッション協会
日本化学繊維協会
一般社団法人 日本金属熱処理工業会
静岡県ソフトウェア事業協同組合
一般社団法人 日本化学工業協会
一般社団法人 情報サービス産業協会
一般社団法人 全日本文具協会
一般社団法人 日本ガス協会
特定非営利活動法人 映像産業振興機構
全国商工会連合会
全国社会保険労務士会連合会
日本ドキュメントサービス協同組合連合会
一般社団法人 日本風力発電協会
日本小売業協会
電気事業連合会
一般社団法人 日本医療機器産業連合会
一般社団法人 日本航空宇宙工業会
特定非営利活動法人 みちのく情報セキュリティ推進機構
独立行政法人 中小企業基盤整備機構
一般社団法人 日本広告業協会
一般社団法人 情報処理安全確保支援士会
一般社団法人 日本電機工業会
一般社団法人 日本印刷産業連合会
一般社団法人 日本自動車部品工業会
一般社団法人 日本鉄鋼連盟
一般社団法人 ビジネス機械・情報システム産業協会
一般社団法人 太陽光発電協会
一般社団法人 日本中古自動車販売協会連合会
特定非営利活動法人 日本セキュリティ監査協会
一般社団法人 電子情報技術産業協会
一般社団法人 日本情報システム・ユーザー協会
一般社団法人 鹿児島県サイバーセキュリティ協議会
一般社団法人 日本工業炉協会
一般社団法人 日本経済団体連合会
一般社団法人 沖縄県情報産業協会
全日本フレキソ製版工業組合
一般社団法人 九州経済連合会
一般社団法人 日本金属プレス工業協会
産業横断サイバーセキュリティ検討会
一般財団法人 関西情報センター
一般社団法人 日本防衛装備工業会
四国ＩＴ協同組合
特定非営利活動法人 山梨ＩＣＴ＆コンタクト支援センター
一般社団法人 保健医療福祉情報システム工業会
せんい強化セメント板協会
一般社団法人 日本自動車機械器具工業会
一般社団法人 全国信用金庫協会
全国カレンダー出版協同組合連合会
一般社団法人 第二地方銀行協会
一般社団法人 日本損害保険協会
一般財団法人 デジタルコンテンツ協会
宮城県サイバーセキュリティ協議会
一般社団法人 中国経済連合会
一般社団法人 日本スポーツ用品工業協会
一般社団法人 日本オンラインゲーム協会
一般社団法人 長崎県情報産業協会
一般社団法人 日本レコード協会
一般社団法人 情報通信ネットワーク産業協会(CIAJ)
公益社団法人 経済同友会
一般社団法人 日本ボランタリーチェーン協会
公益社団法人 日本訪問販売協会
公益社団法人 日本マーケティング協会
一般財団法人 沖縄ITイノベーション戦略センター
公益社団法人 福岡貿易会
大阪商工会議所
公益財団法人 ハイパーネットワーク社会研究所
公益社団法人 関西経済連合会
一般社団法人 組込みシステム技術協会
一般社団法人 オープンガバメント・コンソーシアム
特定非営利活動法人 日本情報技術取引所
全国中小企業団体中央会
日本税理士会連合会
東部大阪経営者協会
一般社団法人 日本医療機器ネットワーク協会
独立行政法人　国立高等専門学校機構
一般社団法人　日本スマートフォンセキュリティ協会
一般社団法人　日本建設機械工業会
ICSCoE叶会
モバイルコンピューティング推進コンソーシアム
一般財団法人草の根サイバーセキュリティ運動全国連絡会
一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG財団）
一般社団法人日本福祉用具供給協会
一般社団法人サイバーセキュリティ連盟
一般社団法人日本建設業連合会

サイバーセキュリティ人材施策の全体像

- 昨年度は、「セキュリティ体制構築・人材確保の手引き」の改訂を行うとともに、セキュリティ人材育成の既存施策を進めつつ、特に、セキュリティを本務としない者が自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につける「プラス・セキュリティ」の取組を推進するため、SC3での検討や地域での具体的な取組を推進。

取組の全体像

セキュリティ対策を進めるための体制・人材の考え方

セキュリティ体制構築・人材確保の手引き（「サイバーセキュリティ経営ガイドライン」付録F）

セキュリティ人材の育成

- ICSCoE中核人材育成プログラム
- 情報処理安全確保支援士
- セキュリティキャンプ

プラス・セキュリティの普及

- SC3産学官連携WGでのプラス・セキュリティ具体化
- NISCにおけるモデルカリキュラム策定
- 地域SECUNITYにおける人材育成

デジタル人材育成プラットフォームにおけるスキル標準の整理・教育コンテンツ・実践型教育

大学・高専等と産業界の連携

今後の方向性

- 手引きの普及による各企業での体制構築の促進と各種セキュリティ人材育成施策を引き続き実施するとともに、プラス・セキュリティの取組を普及させるため、SC3産学官連携WG、デジタル人材育成プラットフォーム、各地域における産学官連携の取組（地域SECUNITY）との連携による取組の具体化・拡大を進めていく。

１．サイバー攻撃の現状

２．経済産業省のサイバーセキュリティ政策の全体像

３．サイバー・フィジカル・セキュリティ対策フレームワーク

４．工場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
ガイドラインの概要および普及啓発

５．工場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
ガイドライン拡充版の検討

「Society5.0」の社会を見据えた対策の検討

- 「Society5.0」では、データの流通・活用を含む、**より柔軟で動的なサプライチェーン**を構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という**新たなリスクへの対応が必要**となる。
- **サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定**し、必要な対策を検討。

サイバー空間で大量のデータの流通・連携
⇒データの性質に応じた管理の重要性が増大

フィジカル空間とサイバー空間の融合
⇒フィジカル空間までサイバー攻撃が到達

企業間が複雑につながるサプライチェーン
⇒影響範囲が拡大

CPSFのモデル

＜3層構造＞

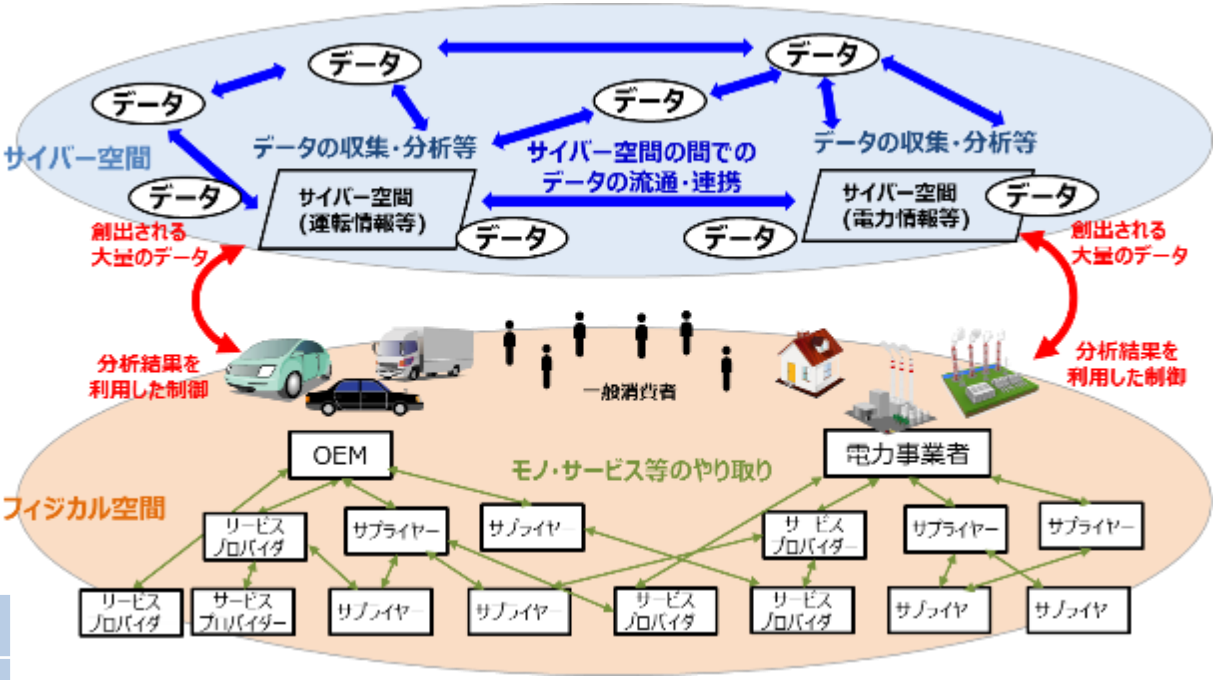
【第３層】
サイバー空間におけるつながり

【第２層】
フィジカル空間とサイバー空間のつながり

【第１層】
企業間のつながり

＜6つの構成要素＞

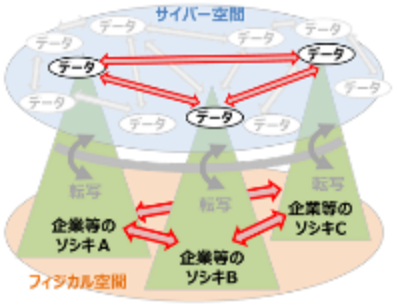
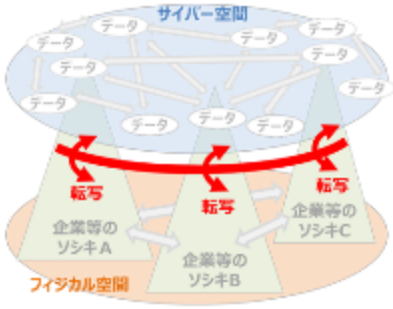
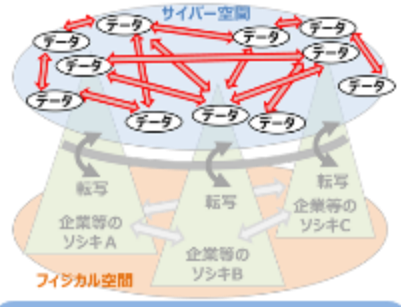
ソシキ	ヒト	モノ
データ	プロシージャ	システム



Society5.0の社会におけるモノ・データ等の繋がりのイメージ

＜CPSFの全体概要＞
三層構造モデルに基づきリスク源、対策要件等を提示

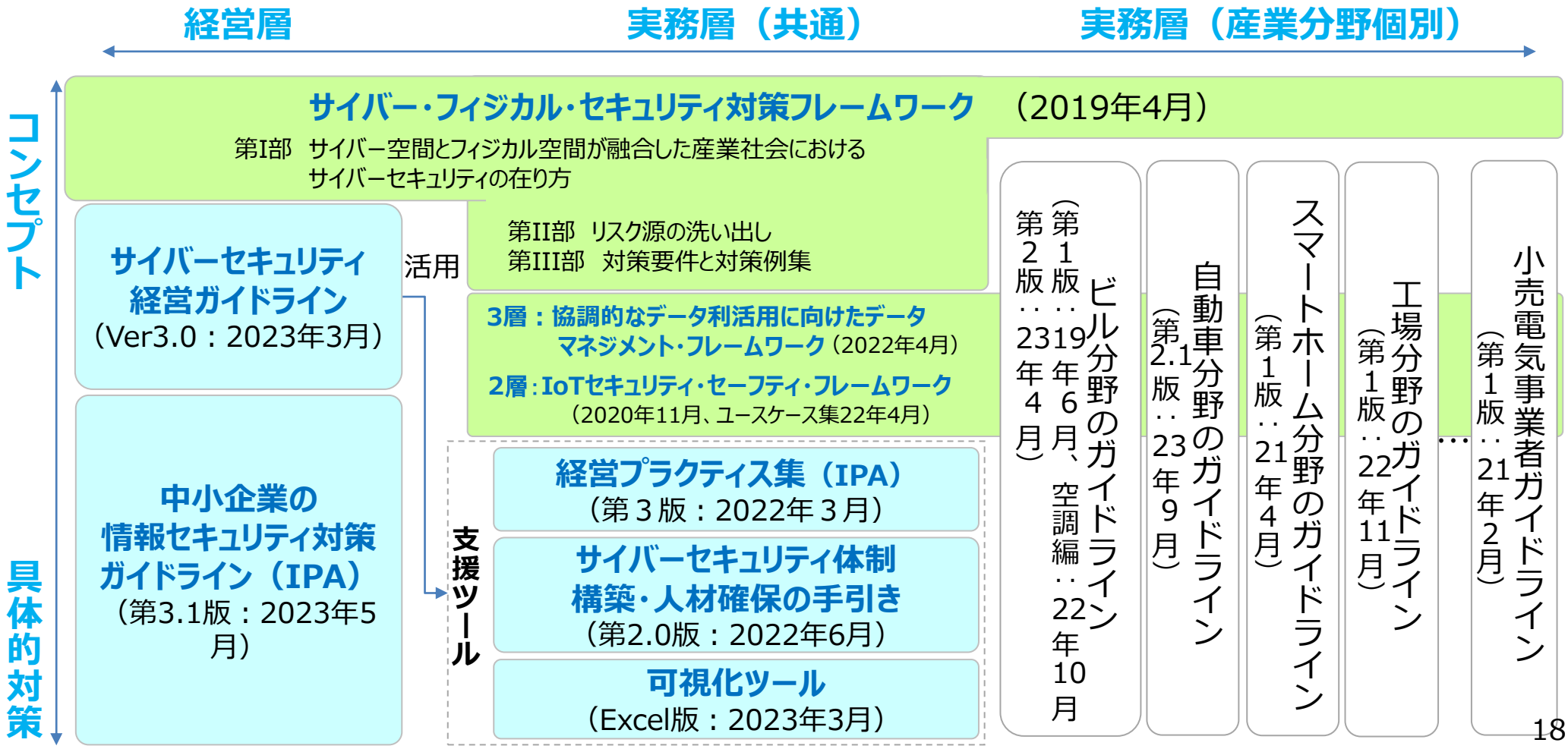
- サプライチェーンの信頼性を確保する観点から、産業社会を３つの層から捉え、それぞれにおいて**守るべきもの、直面するリスク源、対策要件**等を整理。

	企業間のつながり【第１層】	フィジカル空間とサイバー空間のつながり【第２層】	サイバー空間におけるつながり【第３層】
新たなサプライチェーン構造の整理			
機能（守るべきもの）	・平時及び緊急時のリスク管理・対応体制の構築と運用 ・企業内及び企業間のリスク管理・対応体制の構築と運用	・フィジカル空間とサイバー空間の境界における情報の正確な転写及び正確な転写の証明	・データの加工・分析 ・データの保管 ・データの送受信
セキュリティインシデント	・保護すべき資産の棄損 ・他組織のセキュリティ事象発生に起因する事業停止	・不正確なデータの送信 ・安全に支障をきたす動作	・保護すべきデータの漏えい ・なりすまし等による不正な組織からのデータ受信
リスク源（構成要素ごとに整理）	・セキュリティリスクに対するガバナンスの欠如 ・他組織との連携状況の未把握	・不正なIoT機器との接続 ・許容範囲外の入力データ	・通信経路が保護されていない ・通信相手を識別していない
対策要件	■マネジメントルールの徹底 ■関係者との役割分担	■接続相手の認証 ■安全なIoT機器の導入	■暗号化によるデータ保護 ■データの提供者の信頼性確認

サイバー・フィジカル・セキュリティ対策フレームワークを軸とした各種取組

- **<u>「サイバー・フィジカル・セキュリティ対策フレームワーク」では、Society5.0における産業社会でのセキュリティ対策の全体枠組みを提示</u>。**
- 全体の枠組みに沿って、対象者や具体的な対策を整理し、『サイバーセキュリティ経営ガイドライン』や産業分野別のガイドラインなどの実践的なガイドラインを整備。

＜各種取組の大まかな関係＞



１．サイバー攻撃の現状

２．経済産業省のサイバーセキュリティ政策の全体像

３．サイバー・フィジカル・セキュリティ対策フレームワーク

４．工場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
ガイドラインの概要および普及啓発

５．工場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
ガイドライン拡充版の検討

工場SWG （座長：江崎 浩　東京大学 教授）

- 2022年1月6日に工場SWGを設置し、これまでに計6回開催。委員、オブザーバー、ヒアリング対象など、主な関係団体・企業も広く参画し、工場セキュリティガイドラインの策定に向けて活動。
- 2022年11月16日にガイドラインを公表。ガイドラインの拡充版についても検討中。
  https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

開催実績

第１回　工場SWG設置について

第２回　主な産業界団体・企業からのヒアリング
- 日本自動車工業会
- 電子情報技術産業協会半導体部会
- NEC プラットフォームズ
- パナソニック
- 日本鉄鋼連盟
- 日本医療機器産業連合会
- 日本工作機械工業会

第３回　パブコメに向けたガイドライン案の審議

第４回　パブコメ意見を踏まえたガイドライン案の審議

第５回　ガイドラインの普及に関する取組等について

第６回　ガイドラインの拡充版について

委員名簿

江崎 浩（座長）	東京大学 教授
岩﨑 章彦	電子情報技術産業協会
榎本 健男	日本工作機械工業会
桑田 雅彦	日本電気株式会社
斉田 浩一	ファナック株式会社
佐々木 弘志	フォーティネットジャパン株式会社
斯波 万恵	株式会社東芝
高橋 弘宰	トレンドマイクロ株式会社
中野 利彦	株式会社日立製作所
市岡 裕嗣	三菱電機株式会社
藤原 剛	ビー・ユー・ジーDMG森精機株式会社
松原 豊	名古屋大学　准教授
村瀬 一郎	技術研究組合制御ｼｽﾃﾑｾｷｭﾘﾃｨｾﾝﾀｰ
渡辺 研司	名古屋工業大学　教授

Panasonic Cyber Security Team　7

工場(制御システム)のセキュリティ課題

- 長期運用と可用性重視のため、ITシステム同等の対応が困難
  ⇒ 脆弱な状態が前提と考え、侵入されることを前提とした対策が必要
- 制御システムの物理症状からサイバー攻撃の特定は困難
  ⇒ 迅速な対策・復旧には専門家によるサイバー空間での監視が不可欠

問題点	ITシステム（OA用PC）	制御システム（製造システム）	
機器・システムのライフサイクル	3-5年	10年以上	・長期運用 ・OSサポート終了後も稼働
サポート切れOS・ソフトの使用	禁止	禁止できない	・誤動作の可能性あり ・ベンダの保証対象外となる
ウィルス検査ソフト導入	導入必須	導入不可	・誤動作の可能性あり ・専用装置は導入方法無し
セキュリティパッチ適用	適用必須	適用不可	・誤動作の可能性あり ・設備メーカ保証外

JSIA　JEITA 一般社団法人 電子情報技術産業協会 半導体部会

③各社における工場セキュリティを取り巻く課題(1)

➢ 各社ともさまざまな課題を抱えている

- 製造装置は、導入時のシステムのまま使われることが多く、バージョンアップなどセキュリティ対策が実質できない。
- セキュリティ対策ソフトは、装置動作の保証ができないとの装置ベンダーからの回答があり、導入が困難。そのため直接的な保護、検疫ができない。
- 製造装置の保守時に装置や関係するベンダーによるコンピュータウィルスの持ち込みリスクがある。
- 製造装置の修理のためハードディスクなどの記憶媒体を修理に出した際、コンピュータウィルスの混入リスクがある。
- リモート診断・支援などが進む場合、社外からのアクセスに伴うセキュリティ対策をユーザー単独として対策することに限度がある。また、様々なツール、方式が乱立することにより、対応がより複雑になる。
- 導入したセキュリティソリューションにより工場システムへ予期しない影響が発生することがある。
- Cloudベースのセキュリティソリューションでは、自社でコントロールできない問題が発生して、工場のオペレーションに影響を及ぼす。
- 新たな技術/デバイスの登場に対するセキュリティ対策が追い付かない(IoT、Cloud、Mobile etc)。

第2回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化） 工場サブワーキンググループ　資料4-2,4-4より抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/002.html

工場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　～全体概要～

ガイドラインの背景・目的

- 工場のIoT化によるネットワーク接続機会の増加に伴いサイバー攻撃リスクが増加。また、ネットワークの接続に乏しい工場であっても不正侵入者等による攻撃の可能性あり。
- 意図的な攻撃の場合もあれば、たまたま攻撃される場合もある。

→**いかなる工場でもサイバー攻撃のリスクあり**。

- 本ガイドは業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを示した「手引き」。

→**各業界・業種が自ら工場のセキュリティ対策を立案・実行**することで、**工場のセキュリティの底上げを図ることが目的**。

想定する読者の方

- ITシステム部門
- 生産関係部門（生産技術部門、生産管理部門、工作部門等）
- 戦略マネジメント部門（経営企画等）
- 監査部門
- 機器システム提供ベンダ、機器メーカ
  （サプライチェーンを構成する調達先を含む）

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。

対策に取り組む効果

- **工場のBC／SQDC※の価値がサイバー攻撃により毀損されることを防止**。
- セキュリティが担保されることでIoT化や自動化が進み、多くの工場から新たな付加価値が生み出されていくことを期待。

※ 安全確保(S：Safety)、
事業／生産継続(BC：Business Continuity)
品質確保(Q：Quality)
納期遵守・遅延防止(D：Delivery)
コスト低減(C：Cost)

セキュリティ対策企画・導入の進め方

ステップ 1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
- **ステップ1-3**　業務の重要度の設定
- **ステップ1-4**　保護対象の整理
- **ステップ1-5**　保護対象の重要度の設定
- **ステップ1-6**　ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7**　ゾーンと、セキュリティ脅威の影響の整理

ステップ 2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ

(1)システム構成面での対策
① ネットワークにおけるセキュリティ対策
② 機器におけるセキュリティ対策
③ 業務プログラム・利用サービスにおけるセキュリティ対策

(2)物理面での対策
① 建屋にかかわる対策
② 電源／電気設備にかかわる対策
③ 環境(空調など)にかかわる対策
④ 水道設備にかかわる対策
⑤ 機器にかかわる対策
⑥ 物理アクセス制御にかかわる対策

ステップ 3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策

(1)ライフサイクルでの対策
① 運用・管理面のセキュリティ対策
A) サイバー攻撃の早期認識と対処（OODAプロセス）
B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C) 情報共有

②維持・改善面のセキュリティ対策
・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
・組織・人材のスキル向上（教育、模擬訓練等）

(2) サプライチェーン対策
・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

経営者の皆様へ ～ 工場のサイバーセキュリティ対策の推進に向けて ～

工場にサイバーセキュリティ対策が求められる背景

- 工場のIoT化や自動化に伴い工場をインターネット等のネットワークに接続する機会が増加する結果、サイバーセキュリティ上のリスクが増大。また、インターネット接続の機会に乏しい工場であっても不正侵入者等による攻撃を受ける場合もあり。
- **サイバー攻撃は、意図的に狙われる場合もあれば、たまたま攻撃される場合もある**。

- **いかなる工場においてもサイバー攻撃を受ける可能性あり**。
- 特に、一般的に製造業／工場では、**安全確保**(S：Safety)、**事業／生産継続**(BC：Business Continuity)、**品質確保**(Q：Quality)、**納期遵守・遅延防止**(D：Delivery)、**コスト低減**(C：Cost)という価値が重視されているが、**サイバー攻撃はこれらを脅かすおそれがある**。

- **セキュリティの推進は経営層等の意思決定を行う者による体制の構築や適切な指示が重要**。本ガイドラインは、対策を行う実務層向けのものであり、工場のセキュリティ対策を行うにあたり参照すべき考え方や対策のステップを「手引き」として示している。

本ガイドラインの目的

- 各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的。

想定読者

- ITシステム部門、生産関係部門（生産技術部門、生産管理部門、工作部門　等）、戦略マネジメント部門（経営企画等）、監査部門、機器システム提供ベンダ、機器メーカ（サプライチェーンを構成する調達先を含む）

ガイドラインの構成（1. はじめに）

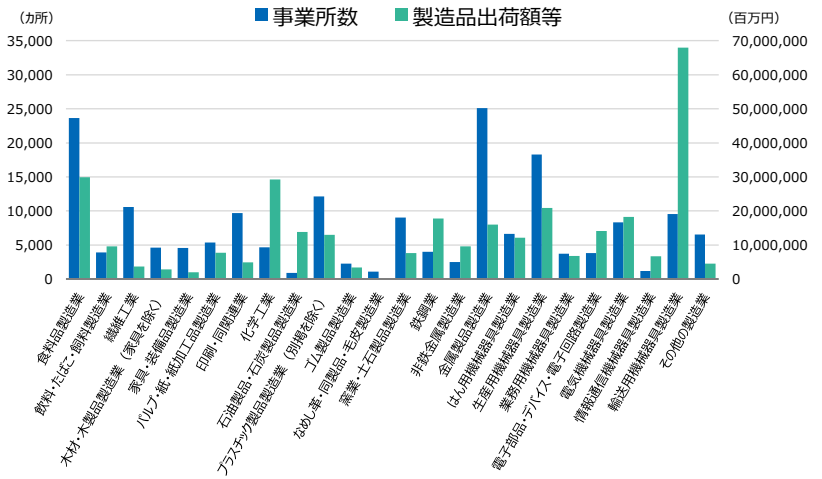
- 「１． はじめに」において、本ガイドラインの目的や想定読者、想定機器・システムを記載。

ガイドラインの目的

- 工場をインターネット等のネットワークにつなぐことによるセキュリティリスクが増加。
- 工場DXに伴い、クラウドやサプライチェーンのシステムと直接接続された工場におけるセキュリティも考慮する必要。
- インターネット接続の機会に乏しい工場についても不正侵入者等による攻撃を受ける場合もある。
- 攻撃の態様により、特定の工場が狙われる場合もあれば、たまたま攻撃した先が工場である場合もある。

したがって、いかなる工場においても、サイバー攻撃を受ける可能性があることを認識する必要がある。

- 一般的に、製造業／工場では、「安全確保(S：Safety)」「事業／生産継続(BC：Business Continuity)」「品質確保(Q：Quality)」「納期遵守・遅延防止(D：Delivery)」「コスト低減(C：Cost)」という価値を重視。
- 工場といっても、業界・業種ごとに実施すべき事項は異なることから、本ガイドラインは**特定の業界・業種や製造する製品という観点で対象を限定したものではない。**
- 業界団体や個社が**自ら対策を企画・実行するに当たり、参照すべき考え方やステップを「手引き」として示し、必要最小限と考えられる対策事項として脅威に対する技術的な対策から運用・管理面の対策までを明記**している。
- 重要なことは、業界団体や個社が、本ガイドラインに示した考え方やステップ、対策を参照しつつ、業界・業種の事情に応じたガイドラインを作成するなどしながら工場へのセキュリティ対策を進めていく、といった行動に移すことである。
- 本ガイドラインは、**各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的**としている。



出所）経済産業省工業統計調査（2020年確報）を元に作成
図 製造業における事業所数・製造品出荷額等（2019年）

ガイドラインの適用範囲

- 本ガイドラインの想定読者は以下を想定。**部門間・担当間の立場や価値観の違いを認識しつつ、コミュニケーション**を行っていくことが重要。
  セキュリティの考え方が経営層（CTO、CIO、CISO等）を始めとした意思決定を行う者に浸透していない場合には、想定読者が適切なコミュニケーションを行うことが重要。
  ■ITシステム部門　■生産関係部門（生産技術部門、生産管理部門、工作部門　等）　■戦略マネジメント部門（経営企画等）
  ■監査部門　■機器システム提供ベンダ、機器メーカ（サプライチェーンを構成する調達先を含む）
- 本ガイドラインの対象機器・システムは、**新設・既設によらず、工場における産業制御システム(ICS/OT)**としており、事務系の情報システム（IT）は対象としない。

ガイドラインの構成（2. 本ガイドラインの想定工場①）

- 工場システムのセキュリティ対策のステップを提示するにあたり、わかりやすさの観点から具体例の1つとしてある工場を想定工場として設定。

  ※読者の置かれた環境と想定工場とが必ずしも一致しない部分もあると考えられるため、読者の置かれた環境に応じ適宜読み替え。

想定企業

- 経営者によってDX(デジタルトランスフォーメーション)が求められている
- 電子機器メーカ
- 複数の拠点に工場が存在し、それぞれの拠点で製品を生産
- 本社が管理する拠点間ネットワークで拠点同士は接続されるが、拠点内ネットワークは拠点ごとに管理
- 工場における有益な情報を見極めて収集、状態を見える化し、得られた気付きを知見・ノウハウとして蓄積

想定組織構成

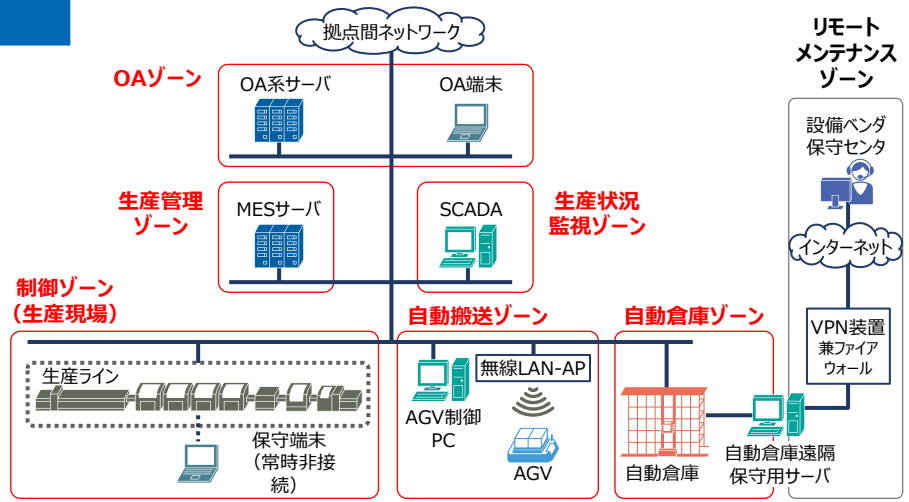
- 生産技術・管理部門
- 工作部門
- 営業部門
- 資材部門
- 品質管理部門
- 情報システム部門

想定生産ライン

- 生産ラインでは電子機器に組み込まれるプリント基板を生産
- 生産自体は自動化されており、生産指示に基づいて複数機種を生産可能
- 段取り掛け、部品の補充などは工場の従業員が実施
- 工場内には複数の生産ラインが存在し、それぞれ独立して異なる機種を生産可能
- 生産設備(装置・機器)は設備メーカから導入し、生産技術・管理部門が生産ラインを構築・管理
- 設備の保守は設備ベンダが実施
- 自動倉庫は、設備ベンダが保守に備えてリモートで状態監視、及び現地での保守を実施

ガイドラインの構成（2. 本ガイドラインの想定工場②）

想定システム、ゾーン



想定業務

- 生産計画設定
- 生産(＋検査)
- 生産状況監視(現場)
- 部材補充(現場へ)
- 部材購入(倉庫へ)
- 生産性分析
- トレーサビリティデータ参照
- メンテナンス
- リモートメンテナンス

想定データ

- 生産計画
- 生産指示(生産機種・量)
- 生産レシピ
- 生産実績(トレサビデータ)
- 設備状態
- 設備プログラム・パラメタ・図面
- 部材在庫量(現場)
- 部材在庫量(倉庫)

工場システム例における構成要素

- ネットワーク
  - 設備系ネットワーク※
  - 生産管理系ネットワーク※
  - 情報系ネットワーク
- 装置・機器（機能・プログラム）
  - VPN装置兼ファイアウォール
  - 無線LAN-AP
  - MESサーバ
  - 生産ライン
  - SCADA
  - 保守端末（常時非接続）
  - AGV制御PC
  - AGV
  - 自動倉庫
  - 自動倉庫遠隔保守用サーバ
  - OA系サーバ
  - OA端末

※近年、設備系ネットワークや生産情報系ネットワークから情報系ネットワークを経由することなく、直接インターネットに接続できる経路も増えているが、そのような場合でも、本ガイドラインに示したステップや対策は活用可能。

※工場といってもその分類や規模は様々であり、機器やシステムも千差万別である。そこで、現場感と矛盾しない効果的な対策が立案できるよう、ある抽象的なモデルから具体的な対策を立案するアプローチではなく、現場の業務から立脚し、工場の機器やシステムを大きな括りの概念として俯瞰的に捉えるためのゾーンを設定し、セキュリティ対策を立案するアプローチを提示している。

ガイドラインの構成（3. セキュリティ対策企画・導入の進め方）

- 工場システムのセキュリティ対策を企画・導入するステップや対策の概略を提示。
- 想定工場に基づき考えられることを例示したものであり、各ステップにおいて、個社や業界ごとに適した整理や考え方の定義を行うことが必要である旨明記。

ステップ 1

内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2** 業務の整理
- **ステップ1-3** 業務の重要度の設定
- **ステップ1-4** 保護対象の整理
- **ステップ1-5** 保護対象の重要度の設定
- **ステップ1-6** ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7** ゾーンと、セキュリティ脅威の影響の整理

ステップ 2

セキュリティ対策の立案

- **ステップ2-1** セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ
  (1)システム構成面での対策
  ① ネットワークにおけるセキュリティ対策
  ② 機器におけるセキュリティ対策
  ③ 業務プログラム・利用サービスにおけるセキュリティ対策
  (2)物理面での対策
  ① 建屋にかかわる対策
  ② 電源／電気設備にかかわる対策
  ③ 環境(空調など)にかかわる対策
  ④ 水道設備にかかわる対策
  ⑤ 機器にかかわる対策
  ⑥ 物理アクセス制御にかかわる対策

ステップ 3

セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策
  (1)ライフサイクルでの対策
  ① 運用・管理面のセキュリティ対策
  A) サイバー攻撃の早期認識と対処（OODAプロセス）
  B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
  C) 情報共有
  ②維持・改善面のセキュリティ対策
  ・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
  ・組織・人材のスキル向上（教育、模擬訓練等
  (2) サプライチェーン対策
  ・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

※重要度については、個社・業界の置かれた環境により様々であることから記載しておらず、個社や業界ごとに適した重要度付けを行うことが重要である。
※なお、重要度付けの考え方については、国際規格等（IEC62443規格群、NIST サイバーセキュリティフレームワーク、IoT-SSF）においても考え方が示されていることから、こうした考え方も参照することが有効である。

ガイドラインの構成（3-ステップ1　内外要件や業務、保護対象等の整理）

ステップ 1

- 工場システムのセキュリティを検討する上で、実施する内容を妥当なものとするために必要な情報を収集、整理する。

ステップ1-1	**セキュリティ対策検討・企画に必要な要件の整理**【3.1.1】	**（1）経営目標等の整理** 工場のセキュリティ対策に関わる経営目標（事業伸張、事業継続等）を整理する。特に、事業継続の観点では、事業継続計画（BCP）が策定されているかが重要であるため、その内容を確認する。BCPが整備されていなければ、必要に応じて担当部署とともに策定の検討を実施する 。 **（2）外部要件の整理** 工場のセキュリティ対策に関わる外部要件（セキュリティ法規制・標準規格・ガイドライン準拠、国・自治体／業界／市場・顧客／取引先／出資者からの要求等）を整理する。 **（3）内部要件／状況の整理** 自社の工場セキュリティに関わる内部要件（システム面、運用・管理面、維持・改善面、等）や体制を整理する。体制等が不明確である場合は、セキュリティ対策を推進するための体制やルール・手順等を整備し実施計画を立案し周知・教育等を実施する 。
ステップ1-2	**業務の整理**【3.1.2】	工場システムが使われている日々の業務の洗い出しを行う。
ステップ1-3	**業務の重要度の設定**【3.1.3】	洗い出した業務について、それぞれの業務の重要度を定める。
ステップ1-4	**保護対象の整理**【3.1.4】	セキュリティ対策を強化すべき業務を支援／実施する工場システムの構成要素(ネットワーク、装置・機器（機能・プログラム）・データ)を洗い出し、システム構成図の模式図を整理する 。
ステップ1-5	**保護対象の重要度の設定**【3.1.5】	事業伸張・継続(BC)、安全確保(S)、品質確保(Q)、納期遵守・遅延防止(D)、コスト低減(C)、それによる業務の重要性の視点から、洗い出した保護対象それぞれの重要度を明確にする。
ステップ1-6	**ゾーンの整理と、ゾーンと業務、保護対象の結びつけ**【3.1.6】	業務の重要度が同等であり、同等の水準のセキュリティ対策が求められる領域として、ゾーンを設定する。ゾーンごとに、これまでに整理した業務、保護対象を結びつける。 ※ゾーンを設定することにより、工場の機器やシステムを大きな括りの概念として俯瞰的に見ることが可能となり、あるゾーン内の保護対象がサイバー攻撃を受けた際、別のゾーンへ影響が及ぶことを抑止し、被害を極小化することを検討することが可能となる。
ステップ1-7	**ゾーンと、セキュリティ脅威の影響の整理**【3.1.7】	最新の脅威について認識した上で、こうした脅威と生産・事業への影響を勘案し、それぞれのゾーンに対するセキュリティ脅威と影響を整理する。

ガイドラインの構成（3-ステップ2　セキュリティ対策の立案①）

ステップ 2

- ステップ１で収集・整理した情報に基づき、工場システムのセキュリティ対策方針を策定する。

ステップ2-1	**セキュリティ対策方針の策定**【3.2.1】	ステップ１で整理したゾーンとこれに紐づく業務、保護対象、想定脅威に対して、業界や個社の置かれた環境に応じ、重要度・優先度を設定する。
ステップ2-2	**想定脅威に対するセキュリティ対策の対応づけ**【3.2.2】	どのようなセキュリティ対策が対応づけられるのか整理する。脅威に対応するためには物理面、システム構成面どちらか一方でなく双方の対策が重要となるため、参照されたい。

（1）システム構成面での対策

① ネットワークにおけるセキュリティ対策（例）

対策項目	セキュリティ強度ごとの対策		
	最低限	中	高
構成分割	–	VLAN等による論理ドメイン細分	物理ドメイン分割
接続機器制限	–	IP、MAC制限	＋接続機器の論理証明 ＋接続機器の信頼性確保
内部秘匿	–	NAT、ステルス	不正通信防止（ゲートウェイ）
通信データ制限	送信元／宛先制限（FW）	＋通信電文種別制限、 ＋電文内容解析・異常検知（IDS）	＋電文内容解析・ 異常通信遮断（IPS）
利用者制限	不要ユーザ削除、パスワードポリシー策定	＋個人ID認証（1要素認証）	＋多要素認証
通信監視・制御	–	通信状況可視化・監視（NDR）、 異常検知（IDS）	＋異常通信遮断 （IPS、フィルタリング）
構成管理	–	接続機器管理・可視化	＋機器内の構成管理・可視化
脆弱性対策	脆弱性情報収集	＋脆弱性診断、侵入可否検査 ＋回避策	＋ソフトウェア更新 （セキュリティパッチ適用） [or 仮想的な対策（IPS、仮想パッチ等）]
ログ取得	機器内ログ取得 （処理負荷への影響を考慮）	＋IDSログ連携	＋ログ分析の仕組み整備

※ 表は例示であり、内容について個社や業界に応じて精査が必要な場合がある。

ガイドラインの構成（3-ステップ2　セキュリティ対策の立案②）

ステップ 2

② 機器におけるセキュリティ対策（例）

対策項目	セキュリティ対策強度		
	最低限	中	高
通信制限	不要サービス閉塞	＋通信先制限	＋FWの導入
不要ポート	端子キャップ	＋ソフト閉塞 （サービスの停止、USBクラス制限等）	＋ハード閉塞（完全に利用不可）
利用ポート	－	持込媒体の検査 （目視や管理票等で外形的に検査）	＋持込媒体のシステムチェック等（ウイルスチェック等でコンテンツやプログラムまでを検査）
通信／接続機器認証	－	IP、MAC、デバイスID認証	＋相手機器の論理証明（暗号による）
送受信データ保護	－	暗号化、暗号鍵の管理	＋暗号鍵の厳密な保護
利用者制限	不要ユーザ削除、パスワードポリシー策定	＋個人ID認証（1要素認証）	＋多要素認証
実行プログラム保護	－	プログラム改ざん対策	＋保護ツール活用
実行プログラム制御	不要プログラム停止・削除、ユーザグループ管理	＋グループ実行権限付与、ユーザ権限動作	＋実行制御ツール活用
ファイル保護	ユーザグループ管理	＋暗号化	＋保護ツール活用
資源保護 (CPU、メモリ、ディスク)	－	定期確認	＋保護ツール活用
構成管理	－	機器内の構成管理・可視化	＋設定情報管理・可視化
脆弱性対策	脆弱性情報収集	＋脆弱性診断、侵入可否検査、 緩和策の適用	＋ソフトウェア更新（セキュリティパッチ適用） [or 仮想的な対策 (IPS、仮想パッチ等)]
ログ取得	システムログ取得 （処理負荷への影響を考慮）	＋操作ログ取得・ログ連携	＋ログ分析の仕組み整備
バックアップ (データ、機器)	－	定期オフライン データバックアップ	＋切替え機器の確保
電源可用性確保	－	UPSの導入	＋自家発電設備の導入

※ 表は例示であり、内容について個社や業界に応じて精査が必要な場合がある。

③ 業務プログラム・利用サービスにおけるセキュリティ対策（例）

パッケージ ソフトウェア	● セキュリティに関する機能仕様が記載されているか ● セキュリティ上の不具合が発生した場合の対応が記載されているか	● セキュリティに関する設定項目の設定値が記載されているか
独自プログラム	● セキュリティを考慮した機能仕様となっているか	● プログラム構築時のセキュリティルールが整備されているか
外部サービス	● セキュリティに関する仕様が提示されているか ● セキュリティ被害の影響に関する取決めが記載されているか	● セキュリティに関する設定項目の設定値が記載されているか

※ 表は例示であり、内容について個社や業界に応じて精査が必要な場合がある。

ガイドラインの構成（3-ステップ2　セキュリティ対策の立案③）

ステップ 2

- ステップ１で収集・整理した情報に基づき、工場システムのセキュリティ対策方針を策定する。

（2）物理面での対策

① 建屋に関わる対策	● 工場建屋は、生産現場を中心に生産設備、自動搬送・倉庫設備、建物設備などを各室に配置した建物であり、その中でも、生産に不可欠な生産システム、自動搬送・倉庫システム、システム間ネットワーク、及びそれらを構成する装置・機器などを、安定的かつ継続的に運用するのに最適な環境及び基盤を提供することが必要となる。
② 電源／電気設備に関わる対策	● 工場・生産設備は、電源の停電・瞬断・電圧変動だけでなく、法定点検、機器の増設・撤去、電源設備・機器の故障などのときにも、製品の生産・品質に影響を与えない、高信頼な電気設備の構築が必要となる。このため、生産設備、自動搬送・倉庫設備などとBAS(ビルディング・オートメーション・システム)とを連動させた設備監視体制の構築、信頼度の高い電源設備構成の構築などが求められる。
③ 環境(空調など)に関わる対策	● 工場の生産ライン、自動搬送・倉庫設備などの環境や、各種システム及びネットワークを構成する機器を設置するサーバ室(計算機室、電算室等)の環境は、空調による冷却、湿度、静電気抑制、空気清浄度などの諸条件を考慮する必要がある。
④ 水道設備に関わる対策	● 工場には、水道がないと稼働しない機器がある。設備に使用する冷却水は、循環式が多く循環が停止すると冷却効率の低下や最悪設備停止に至ることもあることから、例えば、冷却水配管の冗長化、ポンプの冗長化、台数制御にて停止時間を少なくする等の対策を行うことが考えられる 。 ● また、水道設備停止時への対策も必要であり、異常による停止・故障だけでなくポンプ整備などの設備保全時にも停止できるような設計とすることが考えられる。
⑤ 機器に関わる対策	● 工場システムに用いる機器 に対する、設置場所や利用業務の重要性に応じ、また運用面も考慮した上で、セキュリティ対策を行うことが考えられる。
⑥ 物理アクセス制御に関わる対策	● 物理アクセス制御は、生産設備・計算機などの産業制御システム／機器や、それらに付随する情報システムなどへの物理的なアクセスに対する保護を指す。具体的には、産業制御システム／機器の専用室(サーバ室・計算機室)の設置、入退管理システムの導入、監視カメラの設置、管理・監視体制の構築、といった対策が挙げられる。

ガイドラインの構成（3-ステップ3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）①）

ステップ 3

- ステップ3ではライフサイクルでの対策、及びサプライチェーンを考慮した対策を実施する。
- これらの取組により得られた情報により、ステップ3の後は、事業や環境、技術の変化等に応じて計画・対策・運用状況の見直しを行い、必要に応じてステップ1から改めて取組を進めるなどのサイクルを回すことが重要である。

（1）ライフサイクルでの対策

① 運用・管理面のセキュリティ対策

A) サイバー攻撃の早期認識と対処（OODAプロセス）

サイバー攻撃に起因するシステムの異常を早期に検知・把握するために、機器からのアラート、計測値、指示値の挙動などから、通常と異なる兆候に気付き対処する一連の運用業務にサイバー攻撃の視点での監視を加えることが考えられる。また、迅速な対処を実現するために、異常の兆候や問題・被害の発生を想定し、あらかじめ役割・体制や手順を整備しておくことが考えられる。

B) セキュリティ管理(ID/PW管理、機器の設定変更など)

セキュリティ対策を運用する上で必要な管理作業として、下記に挙げるような運用ルールやそれに基づく標準的な手順の作成・実施と、関係者への徹底を行うことが考えられる。

これらの管理を実施していくため、利用者等に対して、機器や媒体の利用や入退室等に関わる運用ルールに関して、周知・教育を定期的に行うことが望ましい 。

なお、ヒューマンエラーへの対策として、セキュリティに関する業務に対する過失や疲労への対策、及びセキュリティに関するルールや意識付け・教育の不備等への対策についても考慮することが望ましい。

C) 情報共有

サイバー攻撃に関する情報の入手を適時に行うことは、個社の適切な備えや効果的なセキュリティ対応につながり、個社が入手したサイバー攻撃に関する情報を業界や政府に提供することは、業界や社会全体でサイバー攻撃から防御することにつながる。

※業種や対象によって入手可能な情報に差があることに留意。こうした状況にあって可能な限り情報を入手・共有するためには、脅威情報や効果的な対策等、各社の対策に資する情報について、業界やコミュニティ等を通じて情報共有を行うことが望ましい。

② 維持・改善面のセキュリティ対策

セキュリティ対策の実施・運用状況とその効果を確認した上で、工場システムを取り巻く環境の変化に関わる情報を収集し、BC／SQDC確保の観点も踏まえて、セキュリティ対策を評価し、必要に応じて物理面、システム面、運用・管理面のセキュリティ対策を見直し、更新する。

ガイドラインの構成（3-ステップ3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）②）

ステップ 3

（2）サプライチェーン対策

- サプライチェーンの広がりとともに、大企業から中小企業までが関わるサプライチェーンの中でも、セキュリティ対策が進んでいない企業がサイバー攻撃によって狙われる事例が増加。
- 対策予算や人材に限りがある中小企業においても、自分たちの事業を守るために工場におけるセキュリティ対策を進める必要。
- グローバル化の進展の中で、サプライチェーンもグローバル化しているため、グローバルなビジネスを行っている企業は、世界情勢の考慮や、各国の法制度あるいは標準規格やガイドライン等に準拠した対策を進める必要。

サプライチェーンにおけるセキュリティリスクは、一つの工場内に閉じずに、エンジニアリングチェーン、サプライチェーン、バリューチェーンの連携先まで影響を及ぼし得ることから、サプライチェーン全体でのセキュリティ対策を検討することが重要。

取引先や調達先への主な確認ポイント（例）

購入製品／部品	● 保守範囲として、セキュリティに関する脆弱性情報や修正プログラムの提供が含められているか ● セキュリティ脅威が発生した場合に、対応できる体制ができているか。また、依頼時に即応が可能な契約形態となっているか ● 当該製品／部品のセキュリティ視点での機能実装、及び検証が実施されているか ● 廃棄時の情報漏えいリスクを考慮した取決めを実施しているか
業務委託	● 従事者に対するセキュリティ要件が明記されているか。また、要件は自社と同等、もしくは、より厳しい内容となっているか ● 従事者に対するセキュリティ教育が実施されているか。また、実施する教育内容は自社と同等、もしくは、より厳しい内容となっているか ● 再委託が許可されている場合、再委託先のセキュリティ管理を行っているか。また、セキュリティ管理内容は、自社と同等、もしくはより厳しい内容となっているか
システム開発受託	● 開発プロセスの各フェーズにおいて、セキュリティを考慮する要件が記載されているか ● 成果物の検収時に、セキュリティ仕様及び実装状況の確認が記載されているか ● 取扱い情報の守秘義務に関する要件が記載されているか ● 委託終了時に、情報を破棄することが記載されているか ● 開発環境に関するセキュリティ要件が記載されているか ● 監査に関する要件が記載されているか
連携システム	● 連携システムを管理する部門と、セキュリティに関する情報を連携することが記載されているか ● セキュリティ障害が発生した場合の責任範囲が記載されているか ● セキュリティ障害が発生した場合に、問題解決に向けた協力内容が記載されているか ● セキュリティ訓練の共同実施が記載されているか ● 共有する情報の取扱いや保護に関する規約や取り決めを定めているか

【参考】付録E　チェックリスト①

- 特に実施いただきたい対策について、具体的な実施内容をイメージし、対策ができているか確認いただくためのチェックリストを5カテゴリ、5段階の達成度で提示。

カテゴリ

- 準備
- 組織的対策
- 運用的対策（システム関連等）
- 技術的対策
- 工場システムサプライチェーン管理

なお、チェックリストの確認項目は例示であり、読者の状況に応じて、項目の追加・削除や、内容の修正を行っても構わない。

達成度

- 各カテゴリに示した対策の達成度を以下の５段階で評価し、工場セキュリティの現状をチェックしていただきたい。

１：未実施
２：一部実施
３：実施済み
４：実施済みで、管理手順を文書化・自動化し、定期的に対策を見直し
５：実施済みで、管理手順を文書化・自動化し、随時見直し

なお、達成度の基準については、読者の状況に合わせて簡素化して用いても構わない。

付録　E-1 チェックリスト

カテゴリ	番号	確認項目	達成度	参照
準備	0-1	工場システムにおけるセキュリティ対策の検討・企画に必要な経営目標、外部要件、内部要件/状況を整理する。		3.1.1 ステップ1-1
	0-2	工場システムにおける業務・保護対象の整理及び重要度の設定を行う。この結果を踏まえてゾーンを設定し、業務・保護対象を結びつけ、セキュリティ脅威との影響の整理を行う。		3.1.1 ステップ1-2 ～ステップ1-7
	0-3	工場システムに関する内外の要件や、業務・保護対象・ゾーン等の情報の収集・整理結果に基づき、工場システムのセキュリティ対策方針を策定し、想定脅威に対する対策の対応づけを行う。		3.2 ステップ2-1 ステップ2-2
組織的対策	1-1	工場システムのセキュリティの必要性について、決裁者（工場長、カンパニー長等）又は経営層が認識を持っており、十分な予算・人員配置などの協力を得られる状態にある。		3.1.1(3) 内部要件／状況の整理
	1-2	工場システムのセキュリティ対応について情報システム部門や生産関係部門等の関係する部署・部門との間で協力・連係態勢が取られている。		3.1.1(3) 内部要件／状況の整理
	1-3	工場システムのセキュリティ検討組織や、担当者が準備されており、責任と業務内容が明確化されている。		3.1.1(3) 内部要件／状況の整理
	1-4	事業継続計画（BCP）が策定されており、工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。		3.1.1(1) 経営目標等の整理 3.1.1(3) 内部要件／状況の整理

【参考】付録E　チェックリスト②

カテゴリ	番号	確認項目	達成度	参照
	1-5	工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの現場教育を行っている。		3.3（1） ライフサイクルでの対策
運用的対策（システム関連等）	2-1	システムが侵害・停止した場合の事業に対するリスクを検討している		3.1.1(1) 経営目標等の整理
	2-2	工場システムにおける専用のセキュリティポリシーが規定されていて、認知されている。		3.1.1(3) 内部要件／状況の整理
	2-3	工場内のシステムからの電子メールやインターネットアクセスはポリシによって禁止している。		3.1.1(3) 内部要件／状況の整理
	2-4	工場システムにおけるセキュリティの異常発生時の責任者の対応が明確化されている。		3.1.1(3) 内部要件／状況の整理
	2-5	工場システムにおけるセキュリティの異常発生時の対応方法を現場作業者が理解し、訓練を実施している。		3.3（1） ライフサイクルでの対策
	2-6	情報資産の検出ツールを利用するなど、工場ネットワークに接続している機器（サーバ、クライアント端末、ネットワーク機器、設備等）の台帳を作成し、システム構成図を作成している。		3.1.4 保護対象の整理
	2-7	工場内に無線LANを導入している場合、ネットワークへの接続を許可された機器の台帳を作成し、無許可の機器を拒否する仕組みがある。		3.1.4 保護対象の整理 3.2.2(1) システム構成面での対策

カテゴリ	番号	確認項目	達成度	参照
	2-8	システムへの侵入を可能とする攻撃手法や脆弱性を特定し、脆弱性へ対応している、又は緩和策を講じている。（脆弱性を特定する手法の例：定期的な脆弱性診断やペネトレーションテスト（侵入可否検査）、組込機器（PLCやIoT機器など）のモデル情報やファームウェア情報の把握及び脆弱性情報の定期的な確認等（※1））		3.2.2(1) システム構成面での対策
	2-9	工場内に外部記録媒体（USBメモリ、フラッシュデバイス）やポータルメディアの利用・持込みに関するルールを定め、運用している。		3.3（1） ライフサイクルでの対策
	2-10	工場内のシステムのパスワードの強度や有効期限等のパスワード設定の考え方を定めたルールがある。（安全に関わる緊急対応を必要とする表示器などの端末は除く）		3.2.2(1) システム構成面での対策
	2-11	工場内のシステムへのアクセス権で使用していない古いアカウント（退職者・異動者など）を速やかに削除している。		3.2.2(1) システム構成面での対策
	2-12	工場ネットワーク内の接続機器について、事前にそれらがウィルスに感染していないことを確認する手順がある。		3.2.2(1) システム構成面での対策
	2-13	システム機能の完全な復旧を想定したバックアップを行い、バックアップデータは保護された場所に格納するとともに、定期的にバックアップデータからの復旧テストを行っている。また、その手順が明確化されている。		3.2.2(1) システム構成面での対策

【参考】付録E　チェックリスト③

カテゴリ	番号	確認項目	達成度	参照
技術的対策	3-1	インストールできる端末にはアンチウィルスソフト又はアプリケーションホワイトリスト（許可リスト）を導入し、インストール不可能な端末では何らかの代替策（USB型のアンチウィルスなど）を導入している。		3.2.2(1) システム構成面での対策
	3-2	アプリケーション／オペレーティングシステム（OS）の重大な脆弱性については可能な限り速やかにセキュリティパッチを適用している。もしくは代替策を講じている。		3.2.2(1) システム構成面での対策
	3-3	端末のオペレーティングシステムの使用サービスやアプリケーションは必要最小限とし、未使用のサービスやポートは停止・無効化している。		3.2.2(1) システム構成面での対策
	3-4	工場の重要設備への物理的なアクセスについてレベル分けなどの十分な対策を行っている（例：監視カメラ、警報装置）。又は、入退室管理、外部の入室者への関係者の付添いなど運用面での代替策を講じている。		3.2.2（2） 物理面での対策
	3-5	工場ネットワーク内において、セキュリティレベルに応じたネットワークセグメント管理を行っている（VLAN等）。		3.2.2(1) システム構成面での対策
	3-6	工場システムのリモートメンテナンスなどを目的とした外部からのインターネットアクセスが可能な場合、認証（２要素認証等）やリモートユーザ毎の接続対象機器（※2）の制限、接続可能時間の制限、メンテナンス期間外の機器接続等の異常検知、ネットワーク侵入防護などの保護対策を行っている。		3.2.2(1) システム構成面での対策
	3-7	工場内のネットワーク（情報システムとの境界やリモートアクセスを含む）の不審な通信を特定するためのネットワーク検知／防護システムを導入している。		3.2.2(1) システム構成面での対策
	3-8	工場内のシステムのログイン、操作履歴などのイベントログを取得している。それらのログは定期的に分析し、必要日数保存している。		3.2.2(1) システム構成面での対策
工場システムサプライチェーン管理	4-1	工場システムのセキュリティ事故発生時に対応ができるよう、制御システムベンダ・構築事業者と連絡・連携体制を構築している。		3.3(2) サプライチェーン対策
	4-2	工場システムのメンテナンス等に関わる協力会社向けのセキュリティ教育を契約開始時及び定期的に実施している。		3.3(2) サプライチェーン対策
	4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダ・構築業者との連絡・連携体制を構築している。		3.3(2) サプライチェーン対策
	4-4	サプライチェーン（協力会社、生産子会社など）における工場システムの脅威、影響度、対応状況（内部及び/または外部監査実施など）を把握できている。		3.3(2) サプライチェーン対策
	4-5	納入される工場システム機器に対して、一定のセキュリティ基準を満たしているかを判定するプロセスや受入検査がある。		3.3(2) サプライチェーン対策
	4-6	新規システム導入時の設計仕様要件にセキュリティに関する要求仕様が明確化されている。		3.3(2) サプライチェーン対策

（※1）テレワークの普及に伴い、VPNを利用して外部から内部ネットワークに接続するケースが増えているが、近年、VPN装置の脆弱性を突いたサイバー攻撃が継続的に見られている。多くは過去に明らかになった脆弱性であり、ベンダからの対策状況も公表されているにも関わらず、多数の被害が出ていることから、自らが利用している工場の機器・システムにおける脆弱性情報の収集・特定を行い、適時に対応することは重要である。

（※2）接続機器の健全性が確保されているか確認した上で、アクセスを許可することが望ましい。

「工場システムのサイバーセキュリティ対策のアンケート調査」概要

- 工場に関連する業界団体を対象に、工場システムのセキュリティに関する対策・課題・要望等を把握することを目的にアンケート調査を実施した。

目的

工場システムを中心としたセキュリティに関する対策・課題・要望等の把握

工場セキュリティガイドラインの普及策の検討

業界団体向けアンケート調査概要

調査対象	経済産業省所管の業界団体 配布対象： パルプ・紙・紙加工品製造業 印刷・同関連業 化学工業 石油製品・石炭製品製造業 プラスチック製品製造業 窯業・土石製品製造業 鉄鋼業 生産用機械器具製造業 業務用機械器具製造業 電子部品・デバイス・電子回路製造業 電気機械器具製造業 情報通信機械器具製造業 輸送用機械器具製造業 非鉄金属製造業
有効回答数	31件
調査項目数	26項目
調査項目	A. 団体の属性情報 B. セキュリティ活動状況 C. セキュリティ課題 D. ガイドライン作成 E. ガイドライン認知状況
調査手法	Webアンケート調査
調査期間	2022年9月～2022年10月

「工場システムのサイバーセキュリティ対策のヒアリング調査」概要

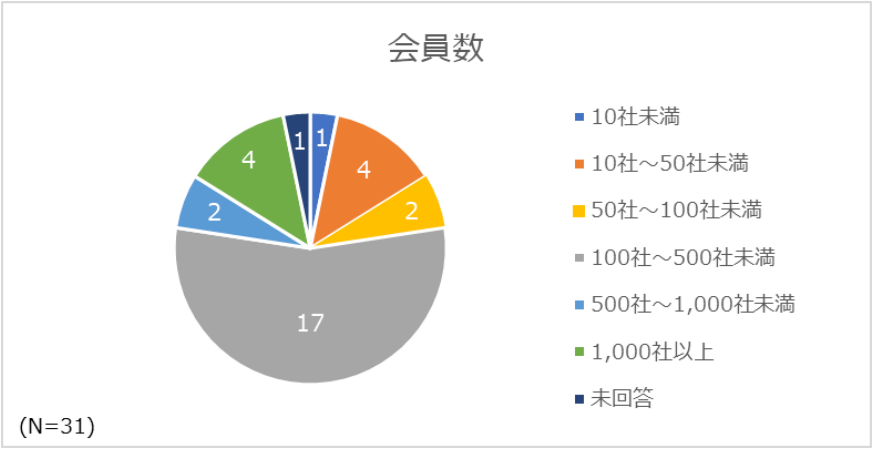
- アンケートに回答いただいた業界団体のうち、セキュリティ活動状況や会員企業のセキュリティ対策状況を考慮し、10団体に対してヒアリングを実施した。
- 業界団体のセキュリティ活動状況、会員企業のセキュリティ対策状況、工場ガイドラインに対する意見、工場ガイドラインの普及活動等について、より具体的な内容を調査した。

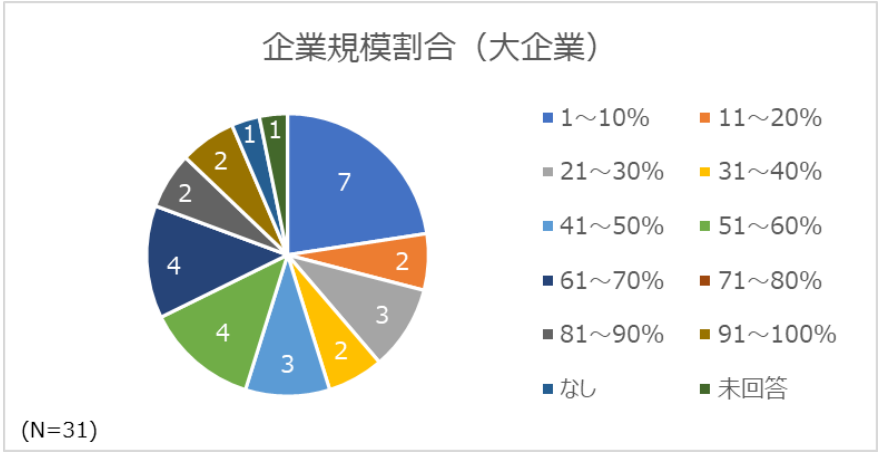
業界団体向けヒアリング調査概要

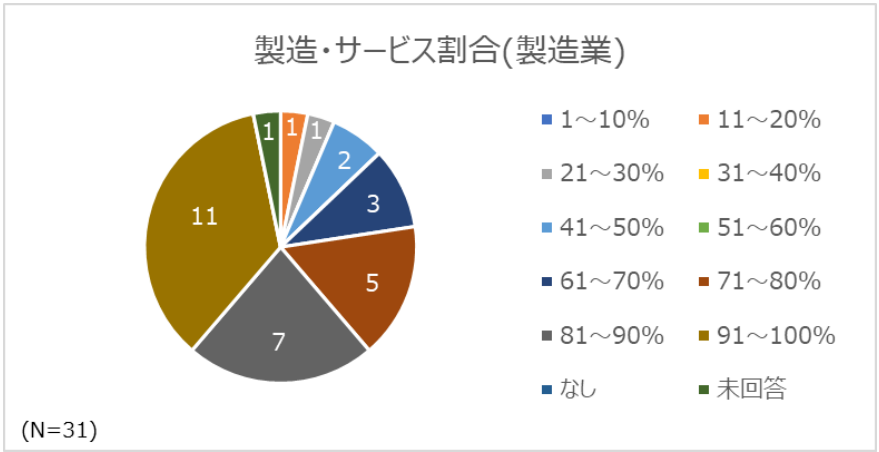
調査対象	経済産業省所管の業界団体
ヒアリング件数	10件
調査項目数	13項目
調査項目	A. 業界団体のサイバーセキュリティ活動状況・展望 （サイバーセキュリティ活動内容・活動経緯・課題・影響など） B. 会員企業におけるサイバーセキュリティ対策状況・展望 （サイバーセキュリティ対策状況・対策の実施理由など） C. 工場セキュリティガイドラインについて （工場セキュリティガイドラインの難易度・活用可能性など） D. 工場セキュリティガイドラインの普及に向けた活動について （工場セキュリティガイドラインの周知や支援策への協力など）
調査期間	2022年12月～2023年2月

（参考）団体の属性情報

- 会員数は、「100社～500社未満」が17団体と最も多かった。
- 企業規模割合（大企業）は「1～10%」が7団体と最も多かった。
- 製造業の割合は、「91%～100%」が11団体と最も多かった。



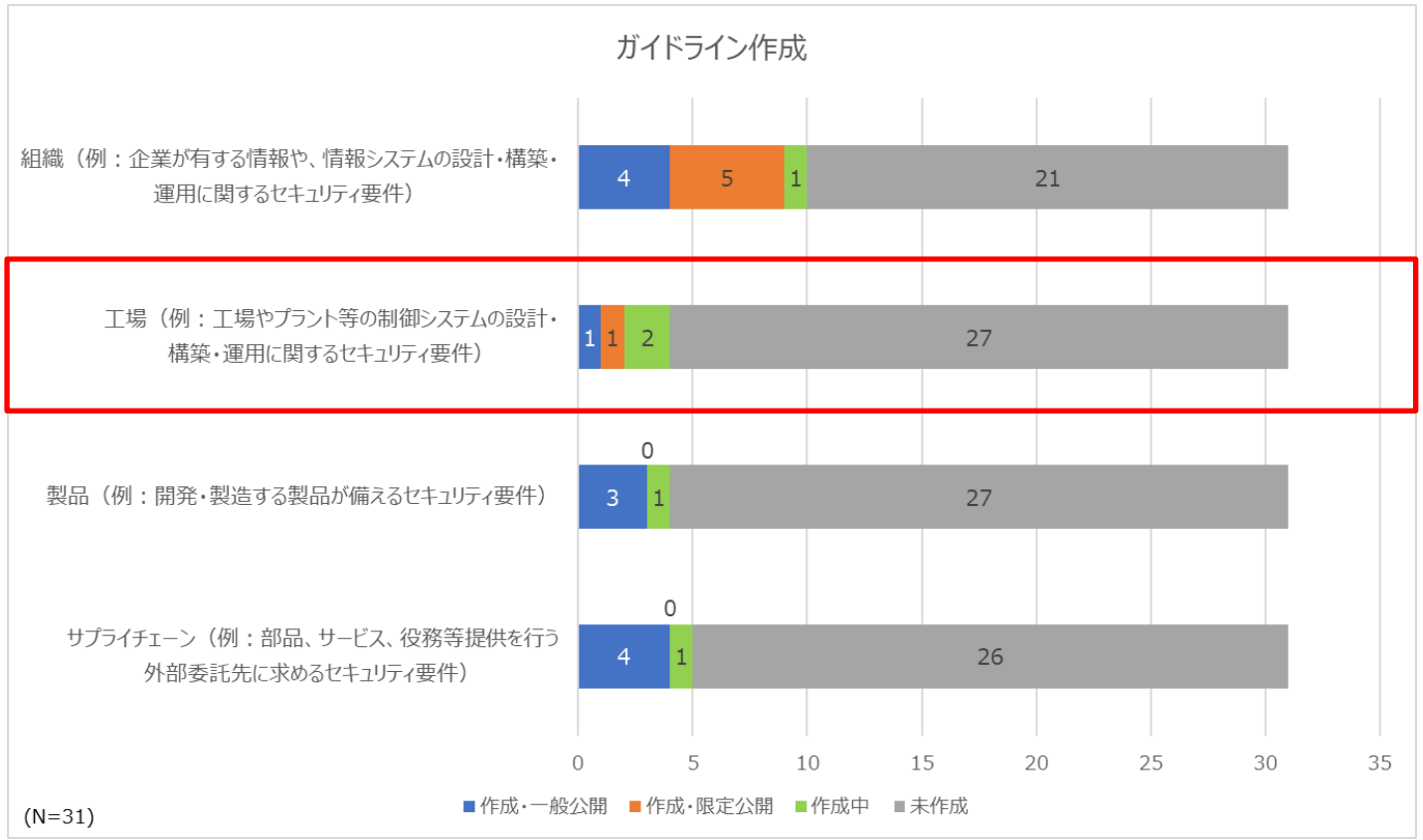




団体向け

業界団体におけるセキュリティガイドライン作成状況

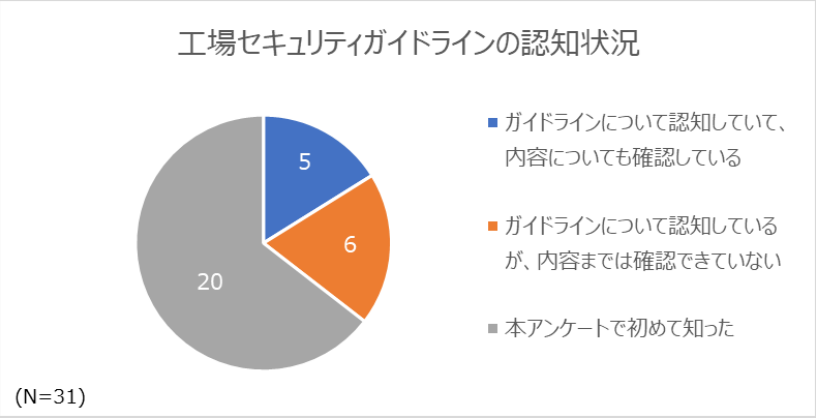
- 「①組織」に関するセキュリティガイドラインについて、「作成・一般公開」、「作成・限定公開」、「作成中」と回答した業界団体は約3割。一方で、「②工場」、「③製品」、「④サプライチェーン」に関するセキュリティガイドラインについて、「作成・一般公開」、「作成・限定公開」、「作成中」と回答した業界団体は約1割。
- 「②工場」は特に作成率が低い。

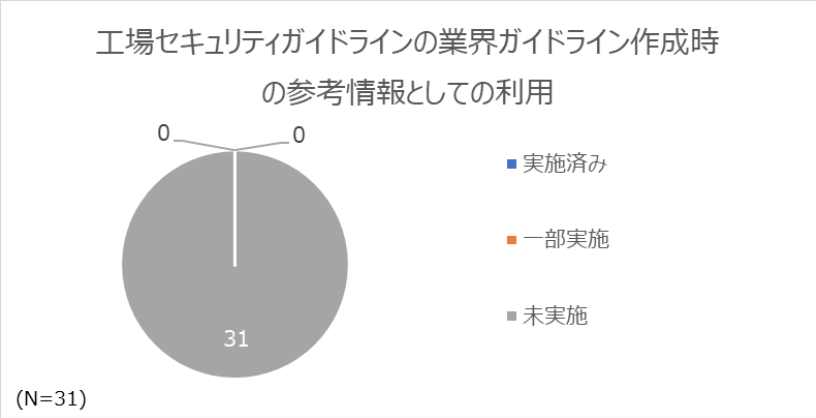


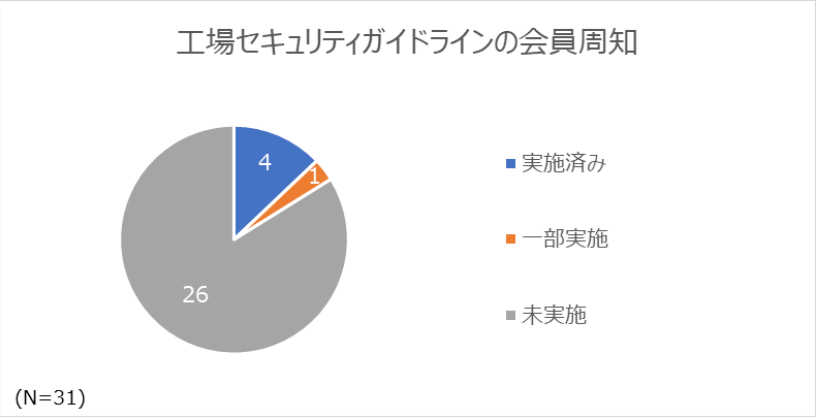
工場セキュリティガイドラインの活用状況

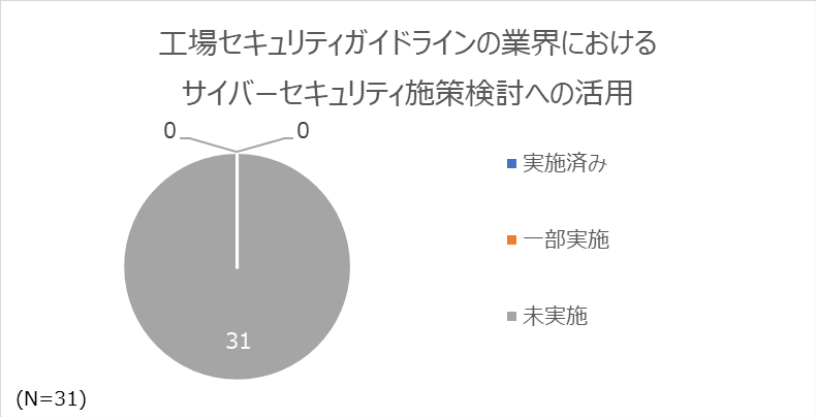
団体向け

- 工場セキュリティガイドラインの認知状況について、「本アンケートで初めて知った」が20団体と最も多かった。
- 工場セキュリティガイドラインの会員周知について、「未実施」が26団体であった。
- 工場セキュリティガイドラインの業界ガイドライン作成時の参考情報としての利用や、業界におけるサイバーセキュリティ施策検討への活用については、「未実施」と全ての団体が回答した。









- 会員周知を「実施済み」と回答した団体が、具体的にどのような方法で周知を実施しているか等を把握する設問は、本アンケートに含まれていない。

会員企業へのアンケート調査概要

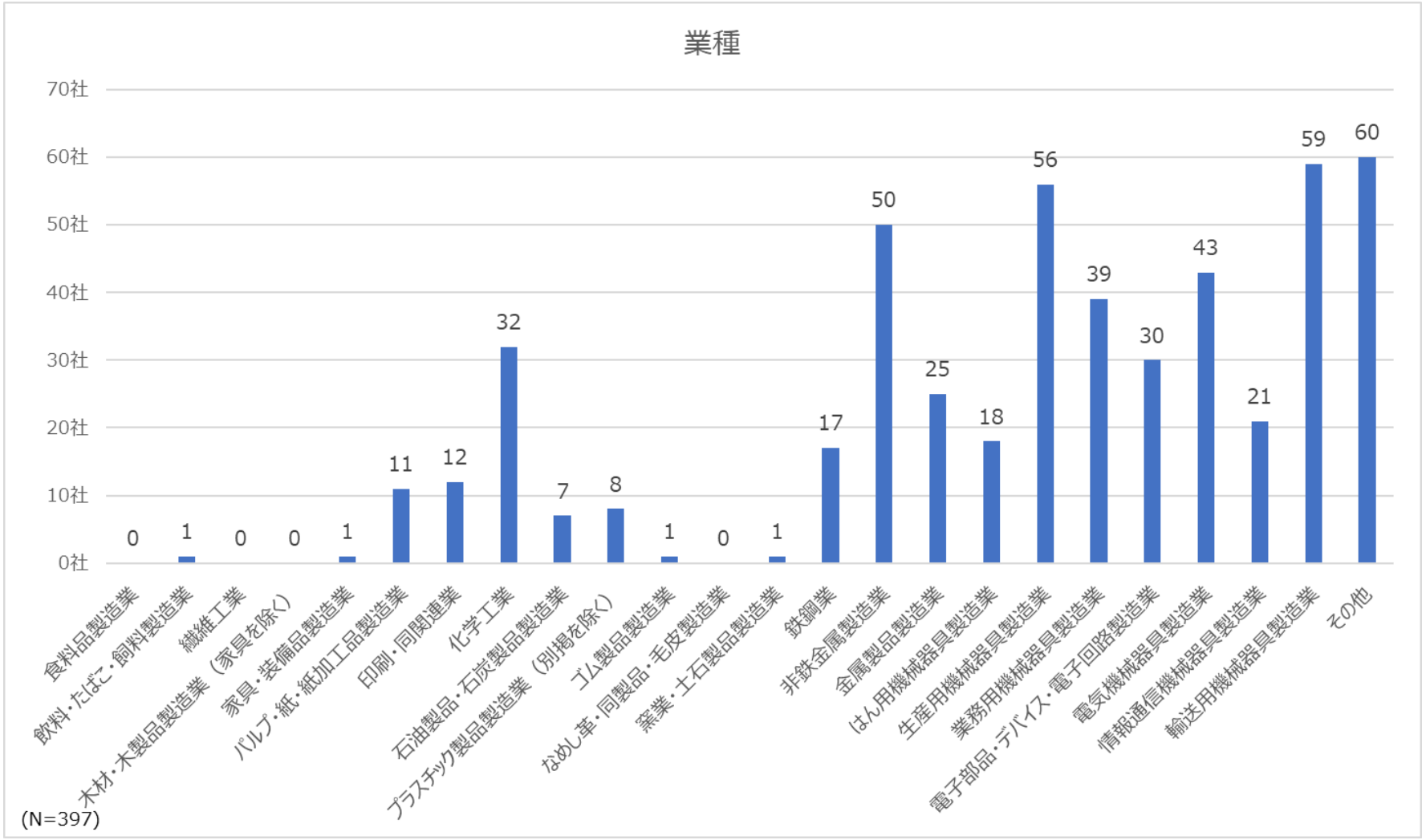
- 業界団体を経由して、会員企業を対象に、工場システムのセキュリティに関する対策・課題・要望等を把握することを目的にアンケート調査を実施した。

調査対象	経済産業省所管の業界団体の会員企業
有効回答数	397件
調査項目数	71項目
調査項目	A. 回答者の属性情報 B. 基本セキュリティ対策 C. セキュリティインシデント D. 工場におけるデータ分析 E. 工場におけるリスク分析 F. 工場におけるセキュリティ体制 G. 工場における外部委託状況 H. 工場における具体のサイバーセキュリティ対策 I. サイバーセキュリティ全般における課題や要望について J. 工場セキュリティにおける課題や要望について K. OSSの対策
調査手法	Webアンケート調査
調査期間	2022年9月～2022年10月

個社向け

（参考）企業回答者の属性情報（1/2）

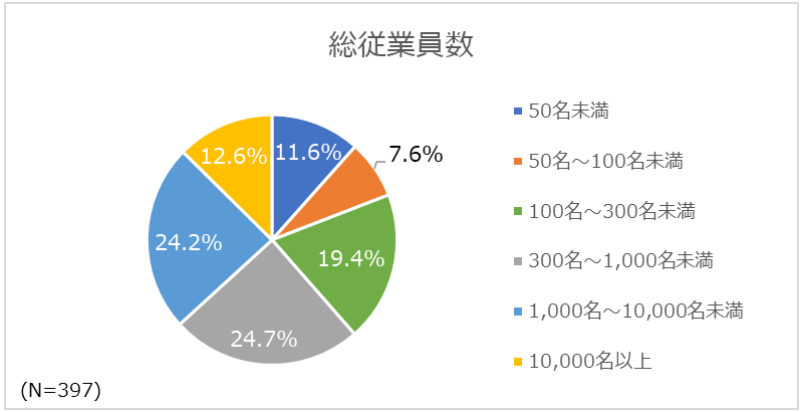
- 業種について、「その他」（60社）が最も多いが、それ以外では「輸送用機械器具製造業」（59社）、「生産用機械器具製造業」（56社）、「非鉄金蔵製造業」（50社）が多い。

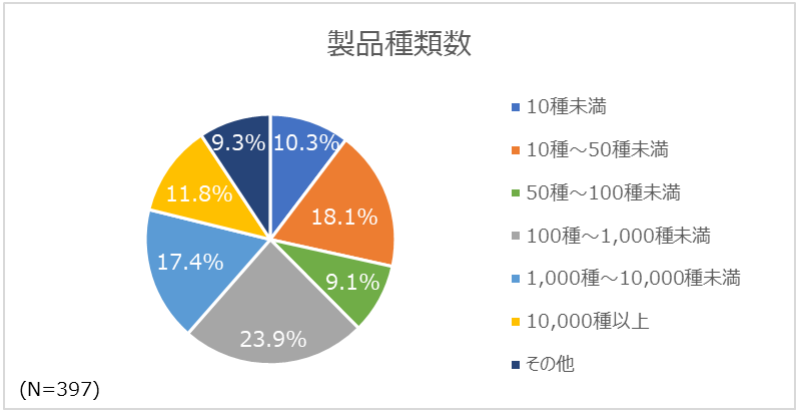


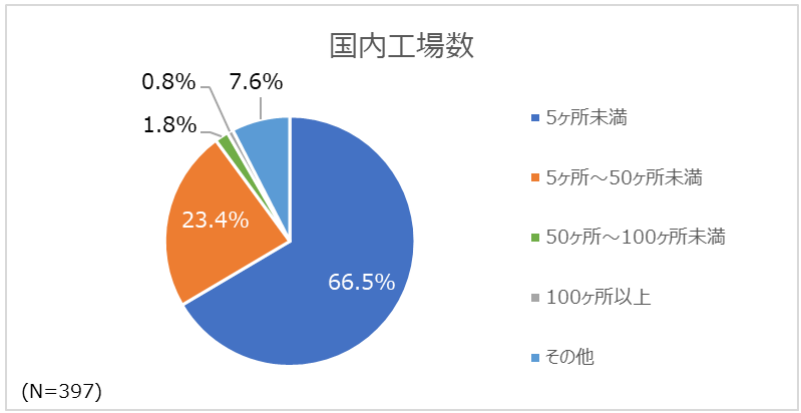
個社向け

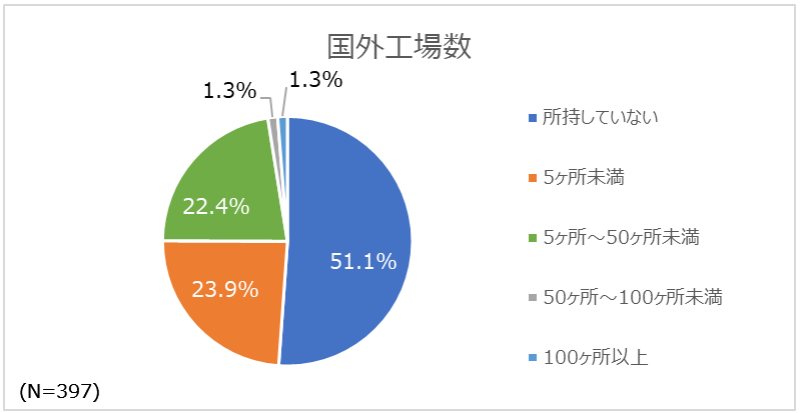
（参考）企業回答者の属性情報（2/2）

- 総従業員数が300名未満と回答した企業は38.6%であった。
  ※中小企業基本法では、「製造業、建設業、運輸業、その他の業種」における中小企業の範囲としては、常時使用する従業員の数が300人以下、と定義されている。
- 取り扱っている製品種類数は、100種未満が37.4%であった。
- 国内工場数について、「5ヶ所未満」が66.5%と最も多かった。
- 国外工場数について、「所持していない」が51.1%と最も多かった。





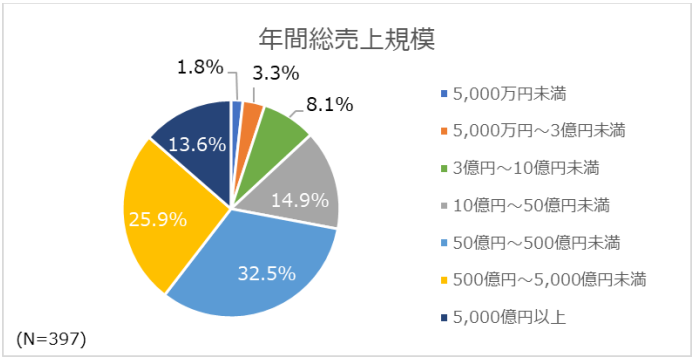


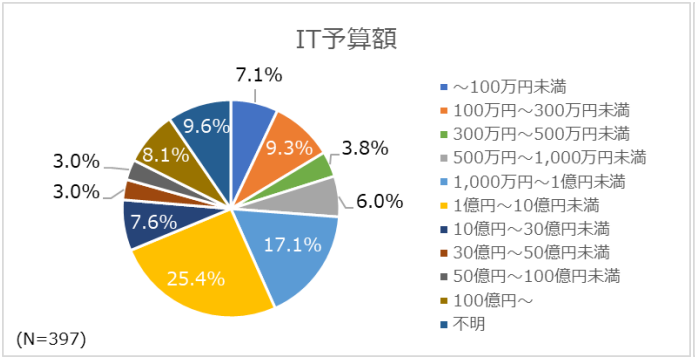


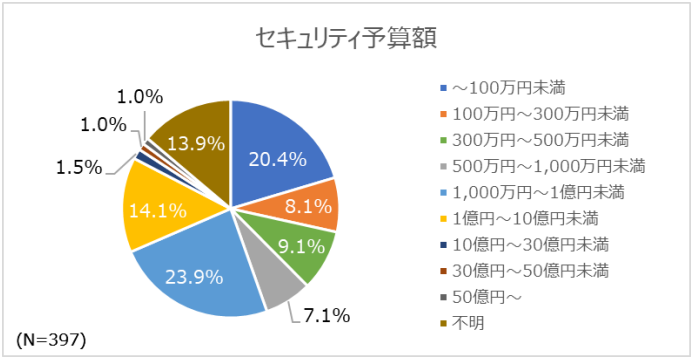
個社向け

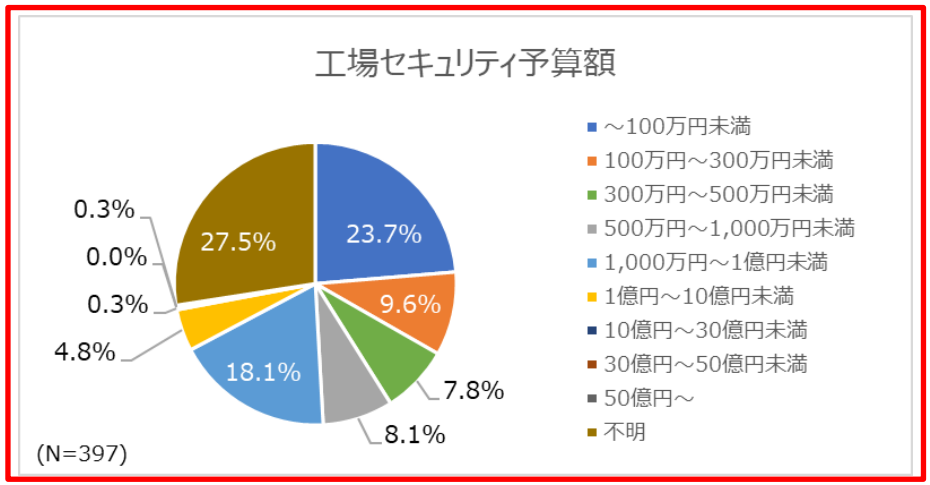
売上規模及び各予算額

- 年間総売上規模が10億円未満と回答した企業は13.2%であった。
- IT予算額は、「1億円～10億円未満」が25.4%と最も多かった。
- セキュリティ予算額は、「1,000万円～１億円未満」が23.9%と最も多く、次いで100万円未満が20.4%であった。
- 工場のセキュリティ予算額は、100万円未満が23.7%と最も多かった。また、不明が27.5%であった。







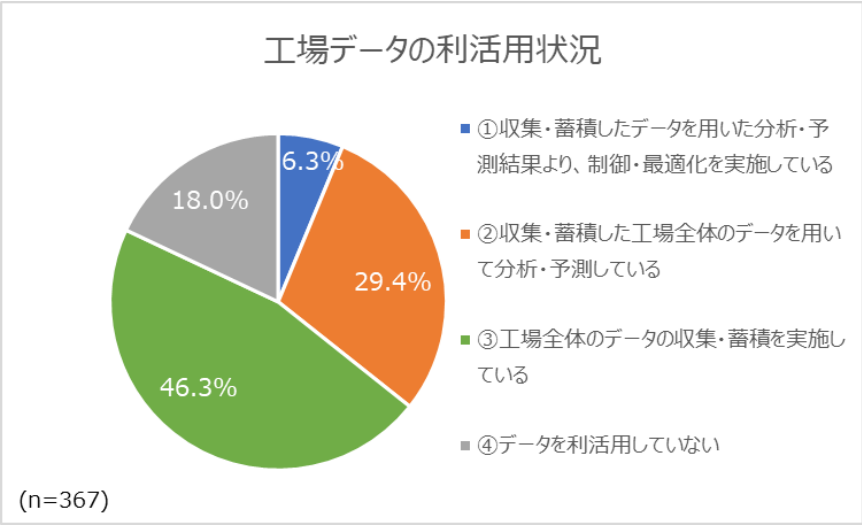


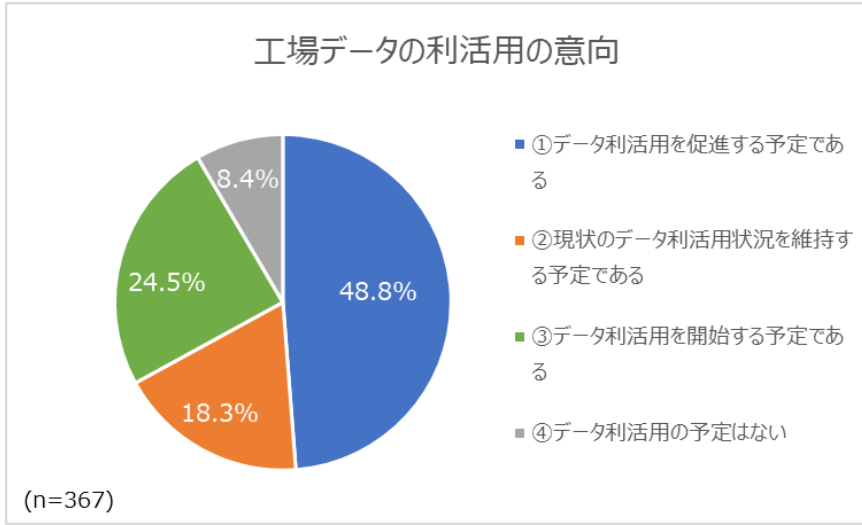
- 工場セキュリティ予算額が「～100万円未満」の企業のうち、**47.9%**の企業が、「工場システムのサイバーセキュリティ予算額が少ない」ことを工場セキュリティの課題に挙げていた。
- これらの企業が具体的にどのような課題認識を持っているかの設問は、本アンケートに含まれていない。
- 「不明」と回答した理由の可能性としては、工場におけるセキュリティ予算額が切り出されていない、本社側で工場側の予算を把握していない、アンケート調査の回答者が企業のITを中心に担当する者であったため把握できていない、等が推察される。

個社向け

工場におけるデータ分析

- 工場データの利活用状況について、「工場全体のデータの収集・蓄積を実施している」と答えた企業46.3%と最も多かった。 一方で、「データを利活用していない」と答えた企業は18.0%であった。
- 工場データの利活用の意向について、「データ利活用を促進する予定である」が48.8%と最も多かった。





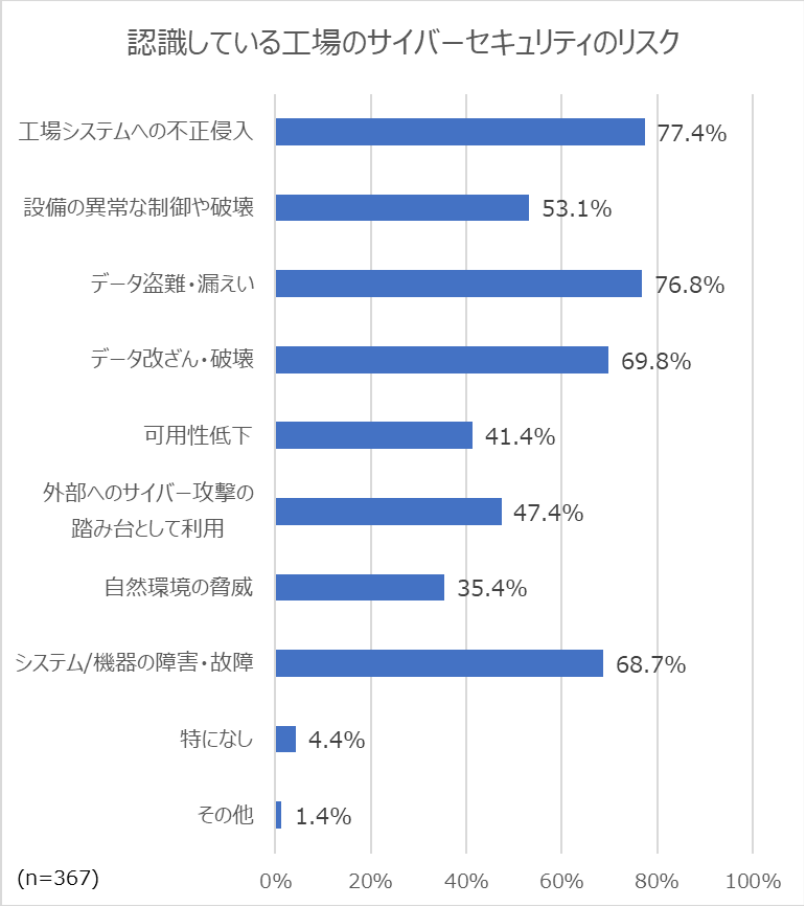
- 各選択肢の例は以下のように示している。
  ① 工場全体のデータを連携できるようデータベース等に保存している
  ② 蓄積しているデータを分析・予測し、生産計画変更や故障予測などに利用している
  ③ 分析・予測結果を基に、工場の各機器をリアルタイムに自動操作などしている
- 回答企業が具体的にどのようなことを実施しているか等を把握する設問は、本アンケートに含まれていない。

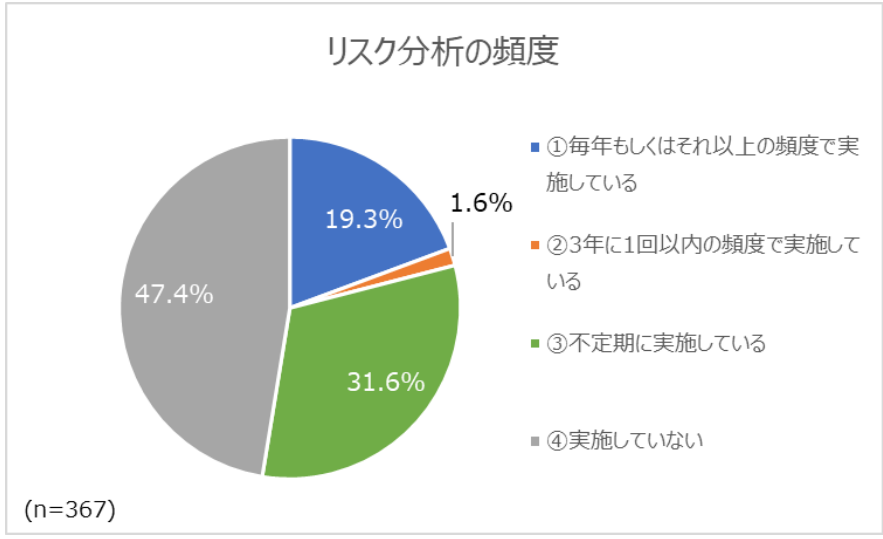
- 回答企業が具体的にどのようなデータ利活用を想定しているか等を把握する設問は、本アンケートに含まれていない。

個社向け

工場におけるリスク分析

- 認識している工場のサイバーセキュリティのリスクについて、「工場システムへの不正侵入」が77.4%と最も多く、「データ盗難・漏えい」（76.8%）、「データ改ざん・破壊」（69.8%）「システム/機器の障害・故障」（68.7%）と続いた。
- リスク分析の頻度について、「実施していない」が47.4%と最も多かった。



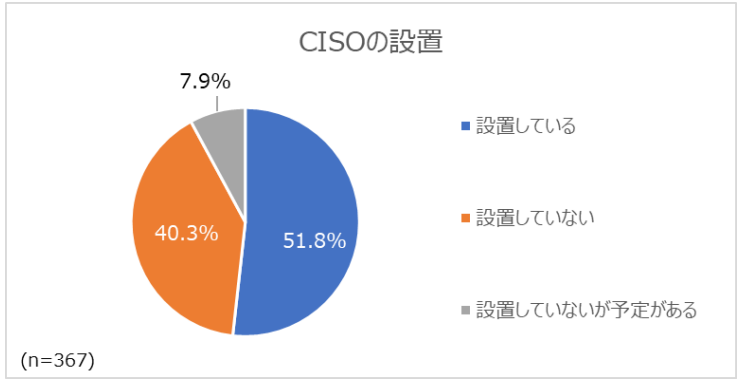


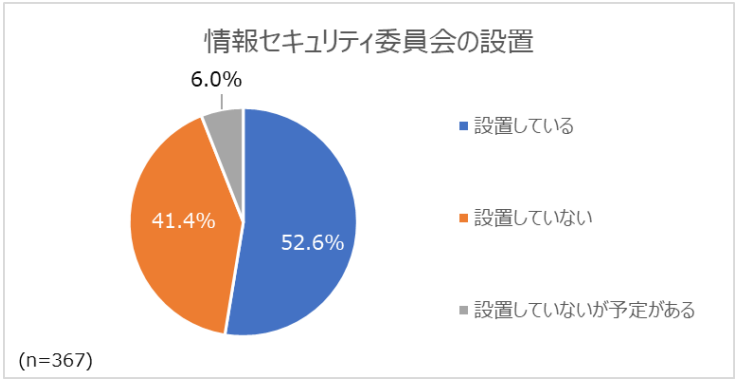
- リスク分析の例として、「リスクが顕在化した場合の事業被害に関する分析」を示している。
- リスク分析の参考資料としてIPAの「制御システムのセキュリティリスク分析ガイド 第2版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～」を示している。
- 回答企業が具体的にどのようなリスク分析を実施しているか等を把握する設問は、本アンケートに含まれていない。

個社向け

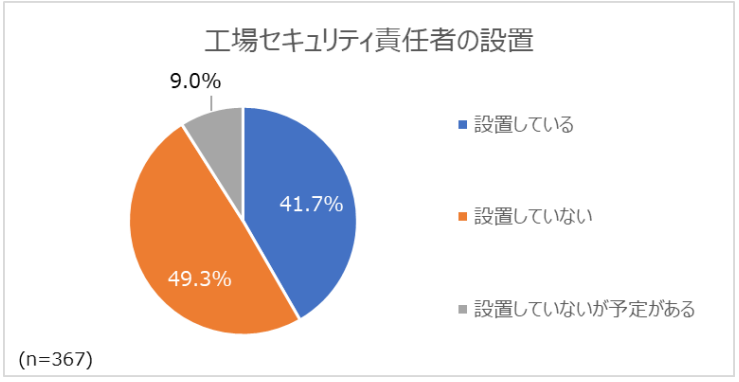
工場におけるセキュリティ体制

- CISOの設置について、「設置している」が51.8%と半数程度だが、工場セキュリティ責任者の設置については、「設置している」が41.7%とCISO設置率より低かった。
- 情報セキュリティ委員会の設置について、「設置している」が52.6%と半数程度であった。





- 回答企業が、情報セキュリティ委員会で具体的にどのような議論を実施しているかや、どのような頻度で議論しているか等を把握する設問は、本アンケートに含まれていない。

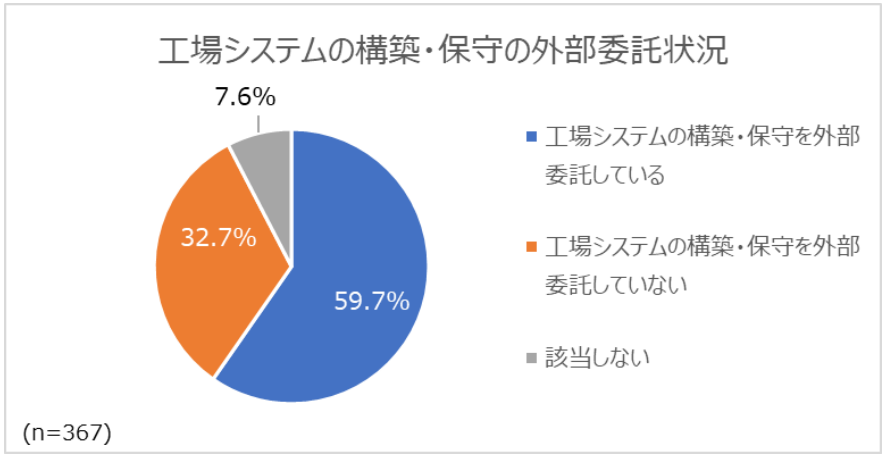


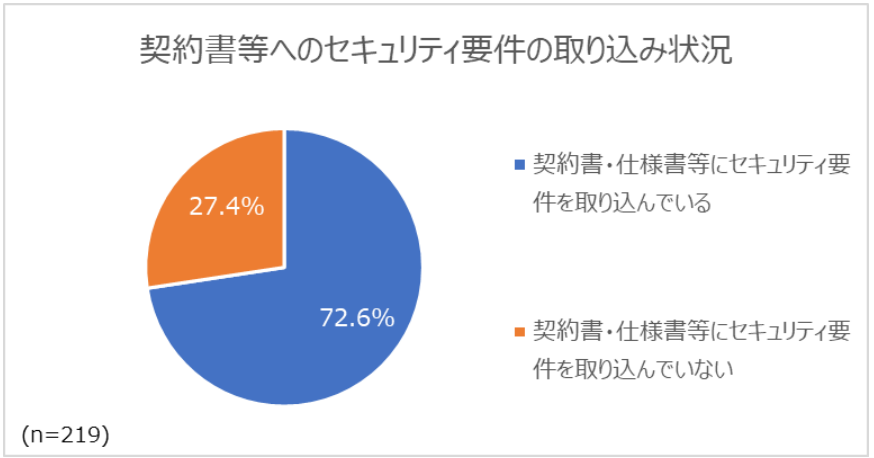
- 回答企業が、工場セキュリティ責任者に具体的にどのような役割を求めているか等を把握する設問は、本アンケートに含まれていない。

個社向け

工場における外部委託状況

- 工場システムの構築・保守の外部委託状況について、「工場システムの構築・保守を外部委託している」が59.7%と約6割は外部委託があった。
- 外部委託のある企業における契約書等へのセキュリティ要件の取り込み状況について、「契約書・仕様書等にセキュリティ要件を取り込んでいる」が72.6%であり、7割以上でセキュリティが考慮されていた。





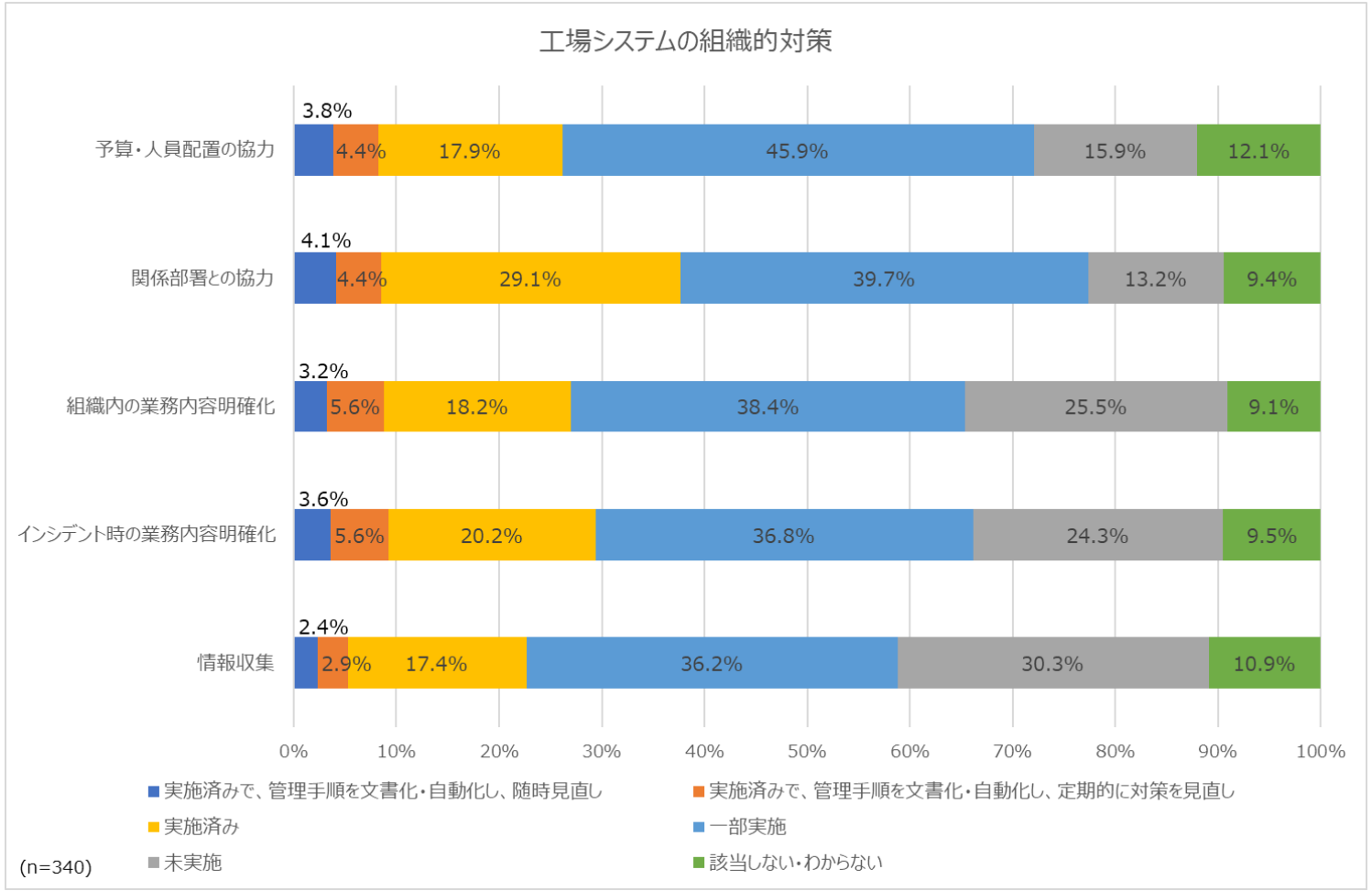
- 外部委託の定義は示していないため、例えば、企業グループ内の外部委託等の場合、「外部委託していない」と回答している可能性がある。

- 具体的にどのような事項を契約書等へ記載したか等を把握する設問は、本アンケートに含まれていない。

個社向け

工場ガイドチェックリストの実施状況（1.工場システムの組織的対策）

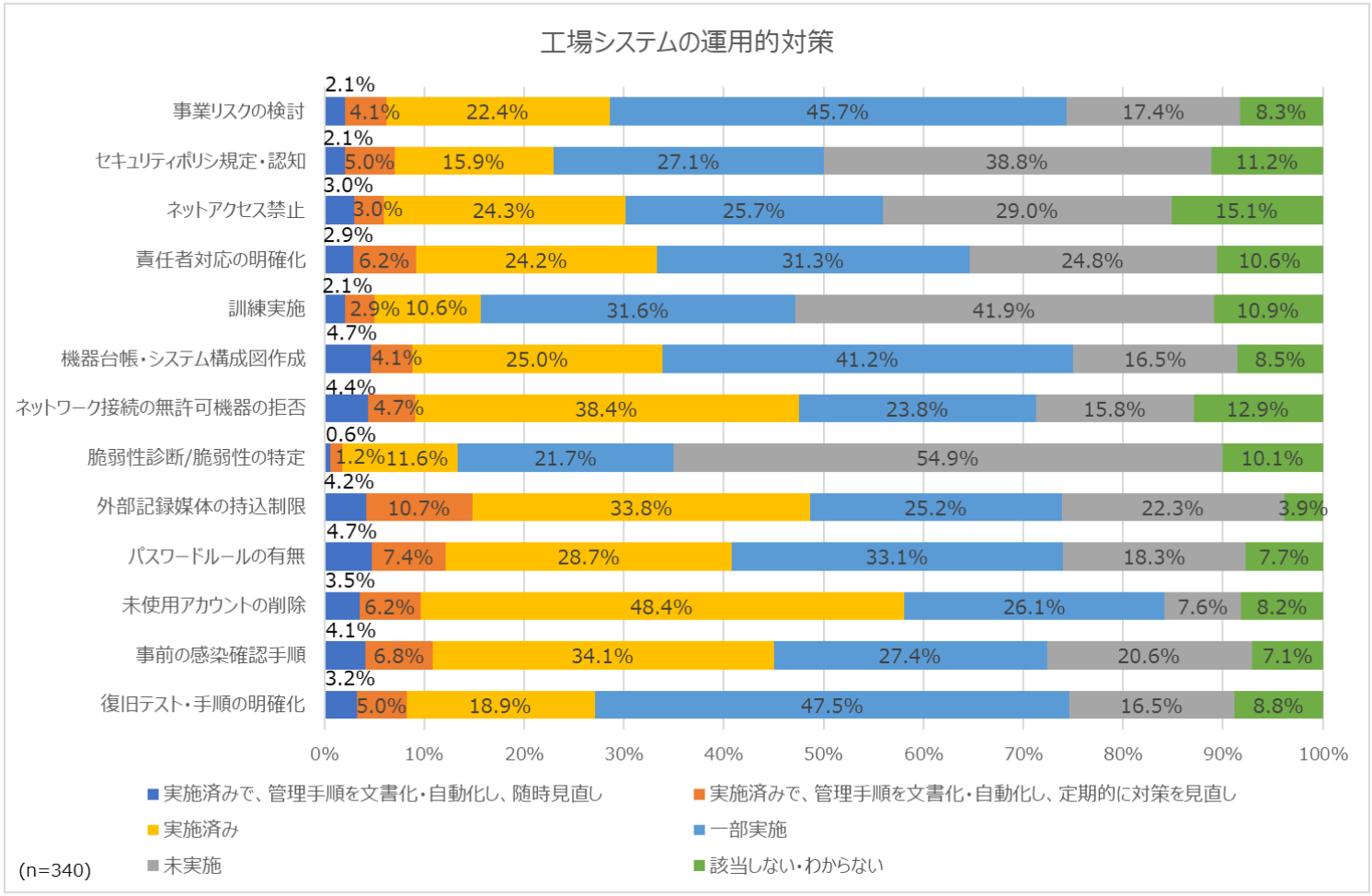
- 工場システムの組織的対策のうち、「情報収集」について「未実施」または「該当しない・わからない」が41.0%と他の対策と比較して、最も多かった。



個社向け

工場ガイドチェックリストの実施状況（2.工場システムの運用的対策）

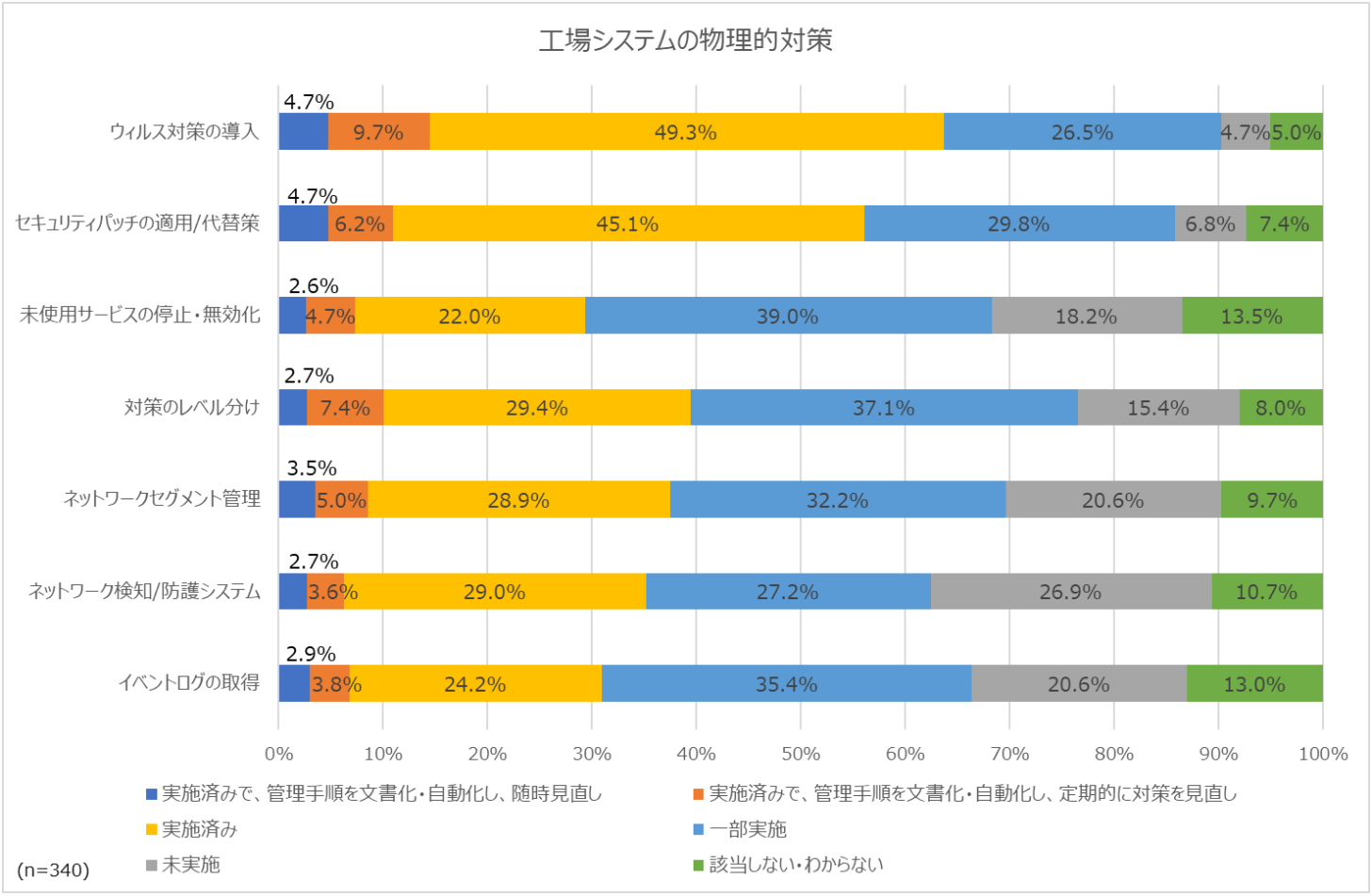
- 工場システムの運用的対策のうち、「脆弱性判断・脆弱性の特定」について「未実施」または「該当しない・わからない」が65.0%と他の対策と比較して、最も多かった。



個社向け

工場ガイドチェックリストの実施状況（3.工場システムの物理的対策）

- 工場システムの物理的対策のうち、「ウイルス対策の導入」「セキュリティパッチの適用/代替策」について実施済み※であるのがそれぞれ63.7%、55.3%と他の対策と比較して多かった。

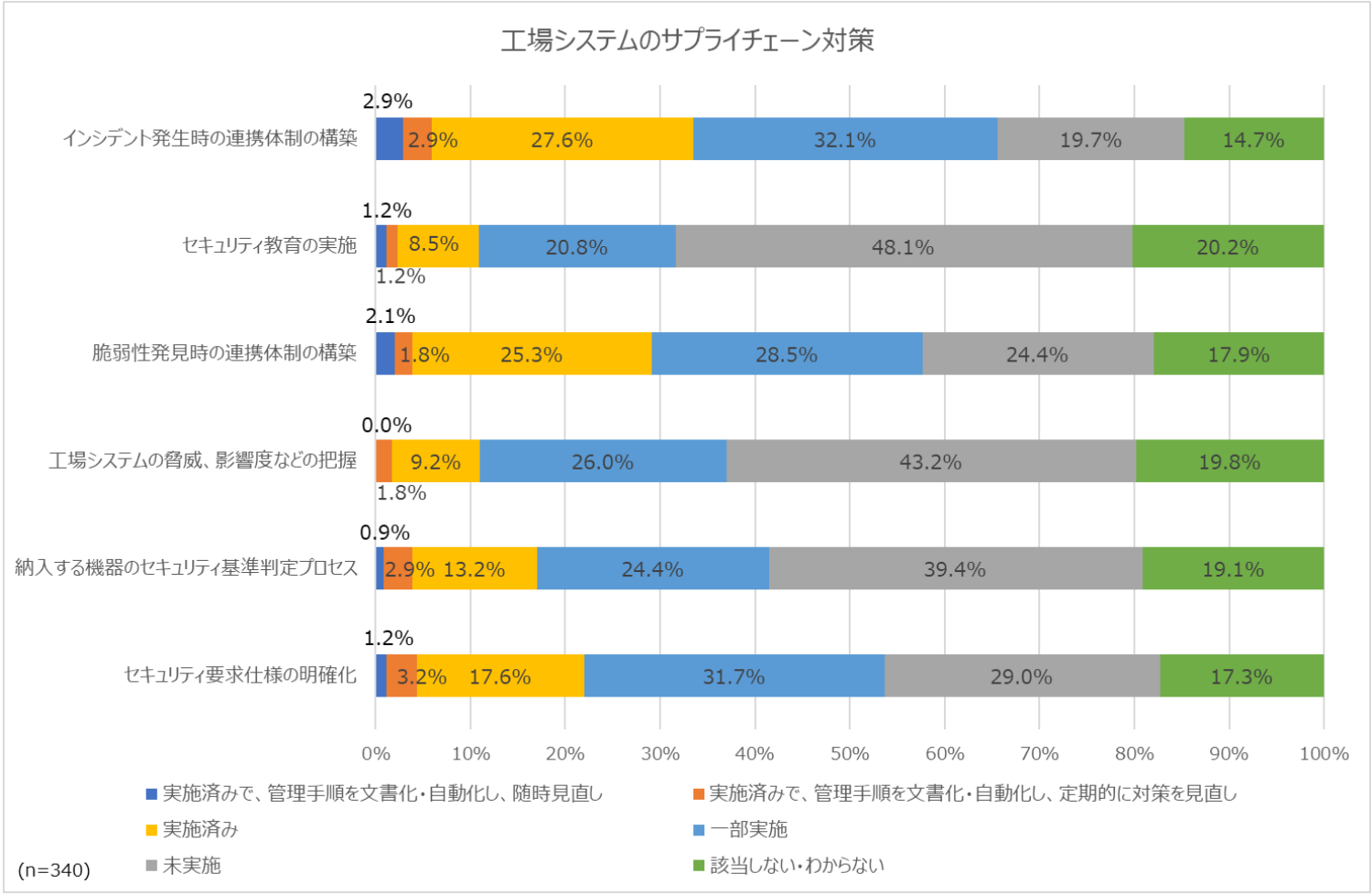


※「実施済みで、管理手順を文書化・自動化し、随時見直し」「実施済で、管理手順を文書化・自動化し、定期的に対策を見直し」「実施済み」の合計

個社向け

工場ガイドチェックリストの実施状況（4.工場システムのサプライチェーン対策）

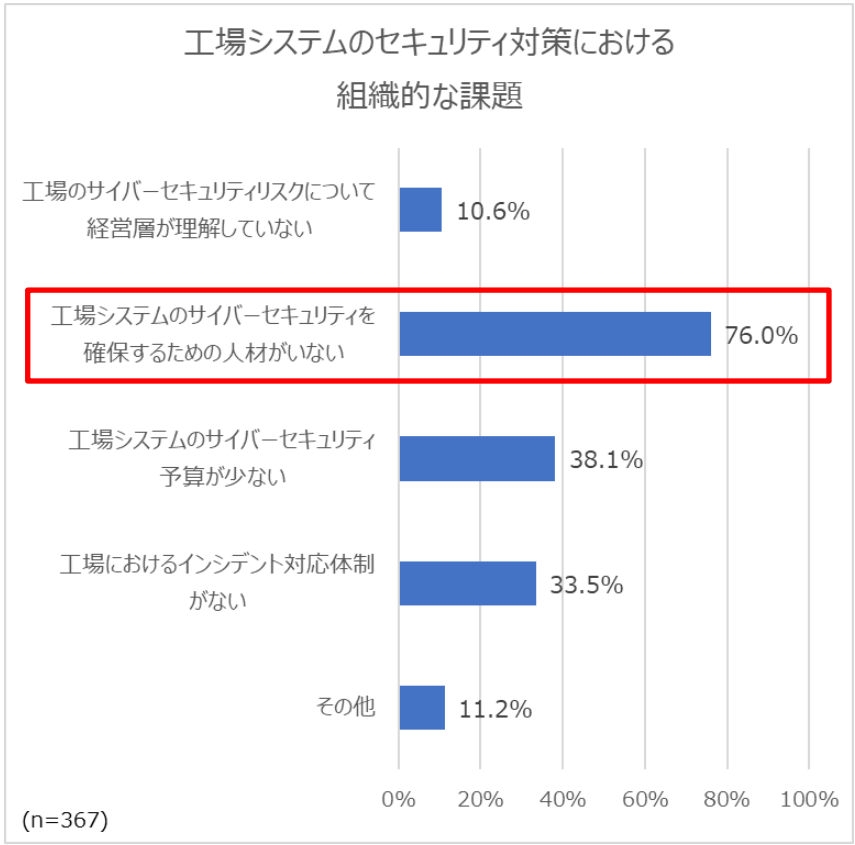
- 工場システムのサプライチェーン対策のうち、「セキュリティ教育の実施」について「未実施」または「該当しない・わからない」が68.3%と他の対策と比較して、最も多かった。

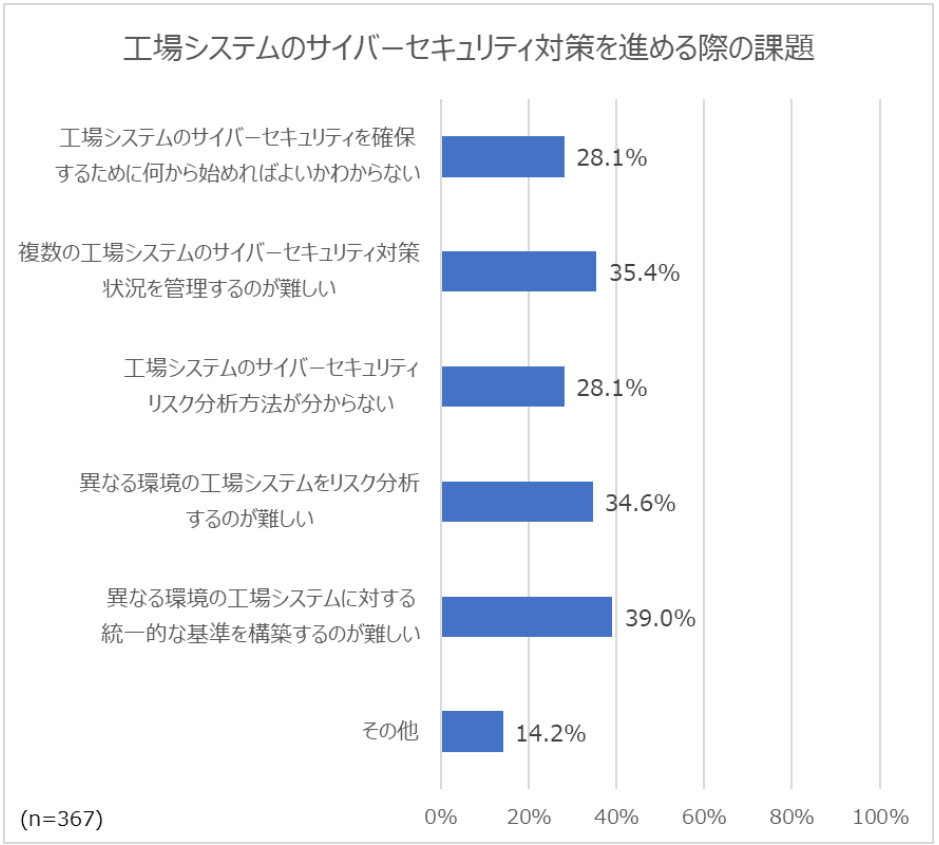


個社向け

工場セキュリティにおける課題や要望について（1/3）

- 工場システムのセキュリティ対策における組織的な課題について、「工場システムのサイバーセキュリティを確保するための人材がいない」が76.0%と最も多かった。
- 工場システムのサイバーセキュリティ対策を進める際の課題について、統一的な基準構築やリスク分析、対策状況の管理の難しさ等、いずれの項目についても3～4割の企業が課題としていた。

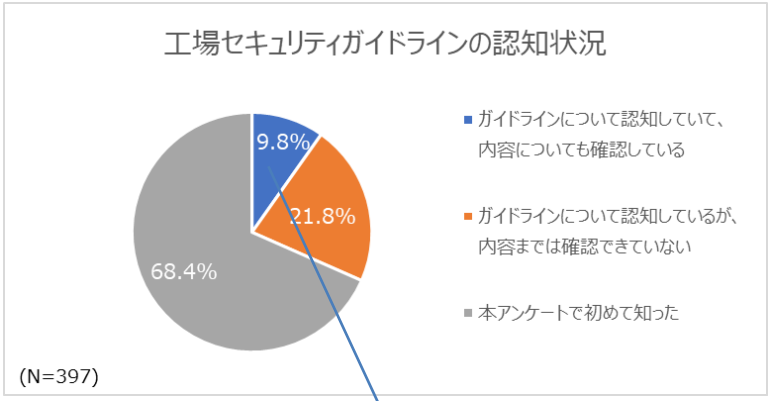


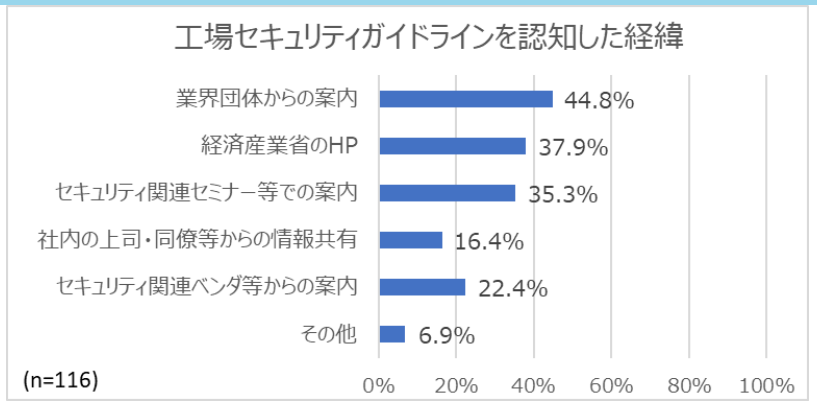


個社向け

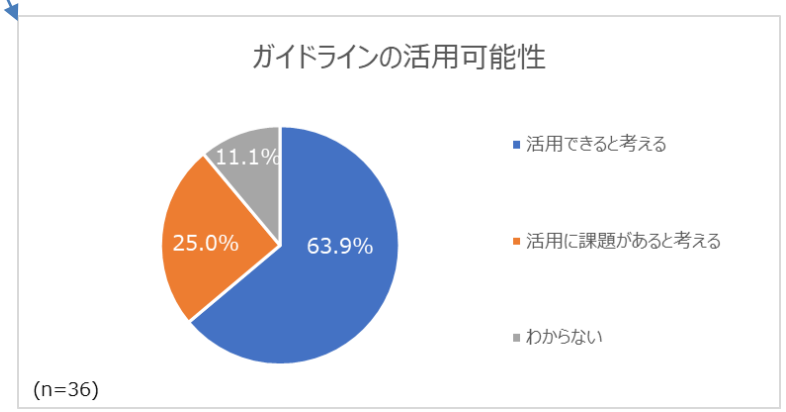
工場セキュリティにおける課題や要望について（2/3）

- 工場セキュリティガイドラインの認知状況について、「本アンケートで初めて知った」が68.4%と最も多く、「ガイドラインについて認知していて、内容についても確認している」のは9.8%であった。
- 工場セキュリティガイドラインを認知した経緯について、「業界団体からの案内」が44.8%と最も多く、「経済産業省のHP」（37.9%）、「セキュリティ関連セミナー等での案内」（35.3%）が続いた。
- ガイドラインの活用可能性について、「活用できると考える」が63.9%と最も多かった。





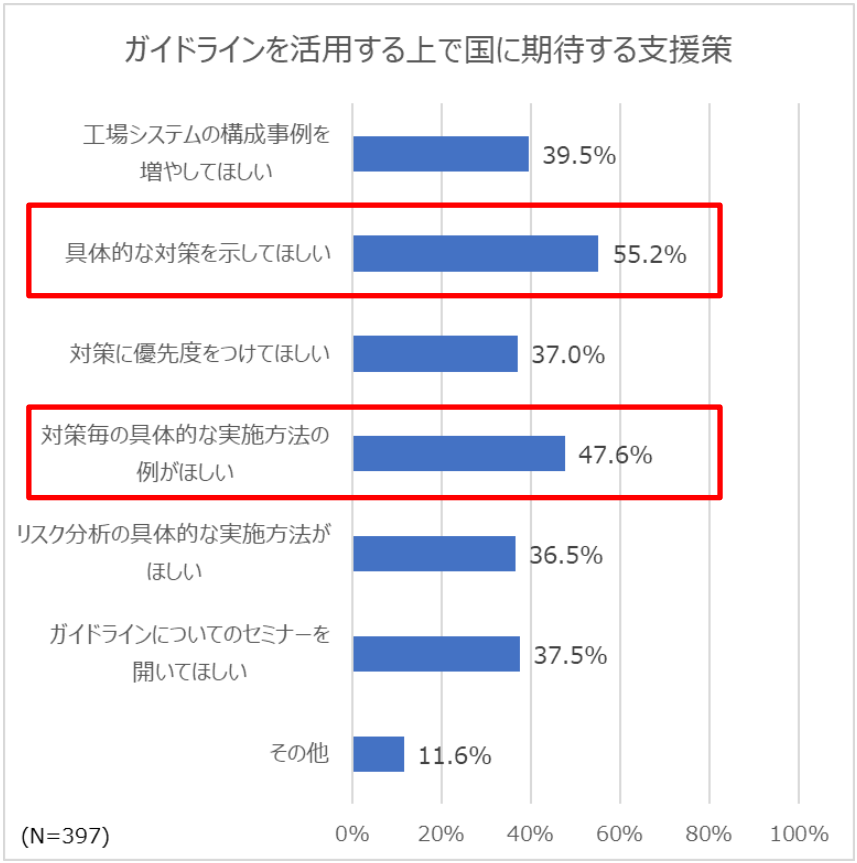
※ 「工場セキュリティガイドラインの認知状況」の設問において、「ガイドラインについて認知していて、内容についても確認している」との回答者が対象

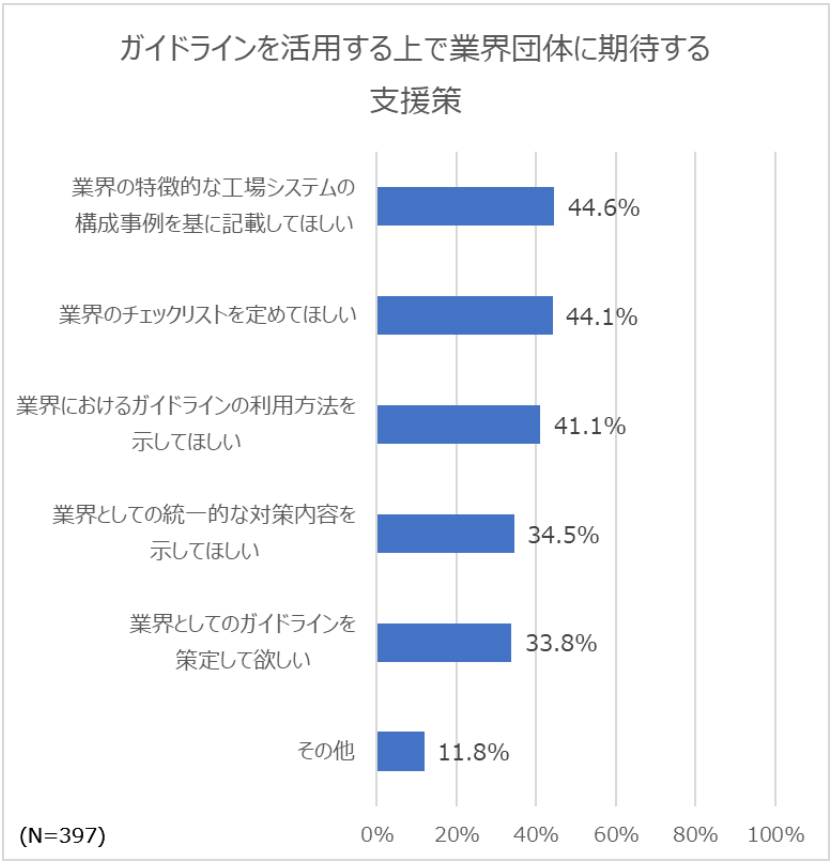


個社向け

工場セキュリティにおける課題や要望について（3/3）

- ガイドラインを活用する上で国に期待する支援策について、「具体的な対策を示してほしい」が55.2%と最も多く、「対策毎の具体的な実施方法の例がほしい」が47.6%と続いた。
- 業界団体に期待する支援策について、業界における構成事例やチェックリスト、ガイドラインの利用方法、統一的な対策内容等、いずれの支援策についても3～4割強の企業が期待していた。

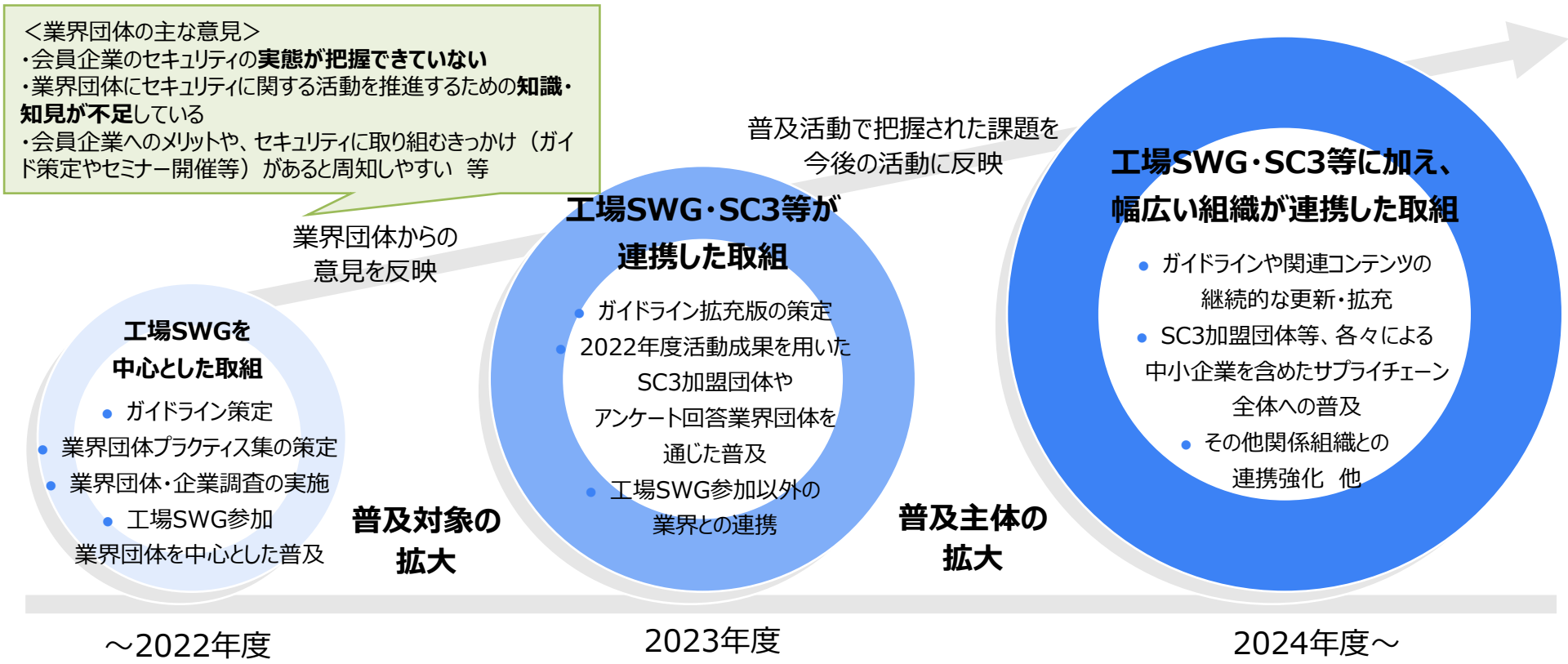




今年度の普及活動と今後に向けた方針

- 昨年度は、業界団体からの意見を踏まえ、企業アンケート調査結果のとりまとめ、及び業界団体のセキュリティ向上活動を整理したプラクティス集を策定した。これらのドキュメントを今年度の普及活動に活用している。
- 今年度の普及活動において業界団体や企業から得られた意見や課題については、今後の普及活動に活かし、工場セキュリティの普及に継続的に取り組んでいく。

普及活動のイメージ

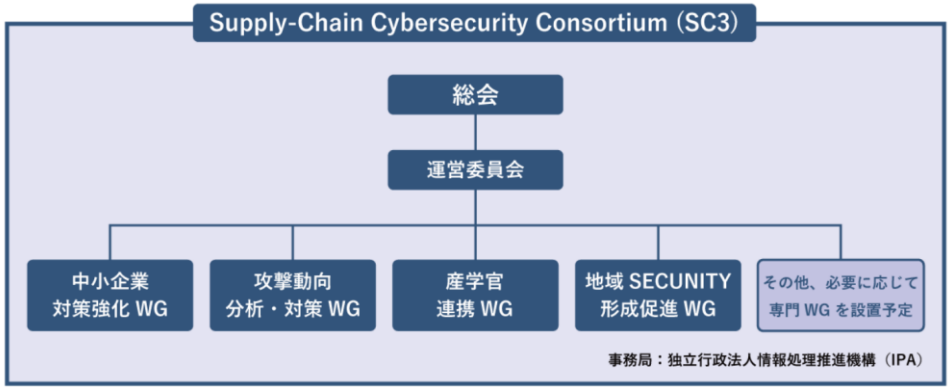


SC3と連携した工場セキュリティの普及活動

- 今年度は、主な製造業に関連する業界団体等（経済産業省工業統計調査の24業種分類を元に抽出した197団体）を対象に、SC3と連携し（1）会員企業へのガイドラインの周知依頼、（2）企業アンケート調査結果及び業界団体プラクティス集の送付を実施する。
- SC3未加盟団体に対しては、SC3の目的や活動紹介を行うことで加盟を促し、SC3を通じてセキュリティ対策推進活動に継続的に関わっていただくことを目指す。

SC3の概要

- **目的**
  産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくこと
- **活動**
  企業のリスクマネジメント強化のための基本的な行動（（1）サプライチェーンを共有する企業間における高密度な情報共有（2）機微技術情報の流出懸念がある場合の報告（3）多数の関係者に影響するおそれがある場合の公表）を促進し、中小企業を含む日本のサプライチェーン全体でのサイバーセキュリティ対策の強化に向けた取組の検討や推進を行う。
- **会員**
  団体を中心とした177者（2023年6月20日時点）



https://www.ipa.go.jp/security/sc3/about/

今年度の普及活動

- **企業アンケート調査結果のフィードバック**
  昨年度に実施した企業における組織及び工場のセキュリティ対策状況や課題等について実態調査結果を提示。
  業界団体の所属企業5社以上回答している場合、業界団体所属企業のみの結果も団体毎にフィードバックを行い、全体との比較ができるよう工夫。
- **業界団体プラクティス集の送付**
  工場セキュリティに取り組む必要性と共に、業界団体におけるセキュリティ向上活動について「情報共有」「ガイドライン等の作成」「人材育成」の3つの観点で活動例を示したプラクティス集を提示。業界団体としての活動に役立てていただくことを想定。

主要な業界と連携した普及活動

- セキュリティ対策に取り組む主要な業界団体等と連携し、工場セキュリティの普及を推進する。

業界	状況
自動車	• エンタープライズ領域を対象とした「自工会/部工会・サイバーセキュリティガイドライン V2.0」を策定済。工場領域についてはガイドライン策定に向けて業界団体において検討中。
半導体	• 半導体製造工場における装置サプライヤー、システムインテグレータ等を対象としたSEMI E187を策定。
鉄鋼	• 「鉄鋼業の制御システムにおけるサイバーフィジカルセキュリティガイドライン第2版」を策定済。
化学	• 「石油化学分野における情報セキュリティ確保に係る安全基準」を策定済。
製薬	• 業界における工場セキュリティに関するガイドラインは存在しない。

普及活動

- 業界団体及び企業へのヒアリング・レビュー結果を、「工場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拡充版」に反映。
- 工場SWGへのオブザーバー参加をはじめ、継続的な情報共有、双方の活動への適宜フィードバックを実施。

IPAと連携した普及活動

- **<u>経済産業省が工場セキュリティに関する方針や枠組みをガイドラインで示し、IPAでは工場セキュリティに関する実施方法や実施例等の文書を公開</u>**。内容については相互参照し、内容の整合性を確保。
- **<u>工場セキュリティに関する取組は、今後も経済産業省とIPAにおいて連携して推進する予定</u>**。

	これまでの取組	今後の取組
経済産業省	 ・「工場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」とチェックリストの公開 ・各種会合等における講演	工場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【別冊：スマート化に向けた対策ポイント】 ・スマート化に向けたガイドライン別冊の作成 ・各種会合等における講演
	参照	
IPA	 ・「制御システムのセキュリティリスク分析ガイド」の公開 ・「スマート工場のセキュリティリスク分析調査」や「スマート工場化でのシステムセキュリティ対策事例調査 報告書」などの工場セキュリティ実装例の調査報告書の公開 ・各種会合における講演やセミナー等の開催	分野別のスマート工場のセキュリティ分析の報告書 ・分野別のスマート工場のセキュリティ分析の報告書の作成 ・各種会合における講演やセミナー等の開催

１．サイバー攻撃の現状

２．経済産業省のサイバーセキュリティ政策の全体像

３．サイバー・フィジカル・セキュリティ対策フレームワーク

４．工場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
ガイドラインの概要および普及啓発

５．工場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
ガイドライン拡充版の検討

スマートファクトリーにおけるセキュリティ検討の必要性

- 現行の「工場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」については、各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的として作成。

・現行のFAシステムを例に、制御システムに対するセキュリティ施策を検討するプロセスおよび勘所を提示

・既存の制御システムを前提に、境界防御型のセキュリティを想定。

ステップ 1

内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
- **ステップ1-2** 業務の整理
- **ステップ1-3** 業務の重要度の設定
- **ステップ1-4** 保護対象の整理
- **ステップ1-5** 保護対象の重要度の設定
- **ステップ1-6** ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7** ゾーンと、セキュリティ脅威の影響の整理

ステップ 2

セキュリティ対策の立案

- **ステップ2-1** セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ
  (1)システム構成面での対策
  (2)物理面での対策

ステップ 3

セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策
  (1)ライフサイクルでの対策
  (2) サプライチェーン対策

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

・スマートファクトリーに向けた制御システムにおけるシステムアーキテクチャの変化

・サプライチェーンによる脅威の増加

工場がクラウドやデジタルツインといったサイバー空間に密接に繋がっていく世界における
セキュリティのあり方を検討することが必要。

スマートファクトリーの目的

- スマートファクトリーは、新たなニーズへ対応した商品やサービスの迅速な提供を実現できるなど、 製造業のビジネス競争力を強化する源泉。
- 工場のスマート化を達成していくためには、汎用品の活用、クラウドとの連携やデジタルツインといったサイバー空間との密接な繋がりが進んでいくと想定される。

DXによるビジネス競争力の強化

新たなニーズへの対応・創生

周辺・活用ビジネス
・既存ビジネスカテゴリー
・商品
・サービス

融合ビジネス
・他社
・商品
・サービス

企業競争力の確保

アジャイル型ダイナミックライン
・分析フィードバック
・他社連携
既存製造ライン

リモート、集約
・人員集約
・場所フリー
現場での作業

DX技術を活用した生産現場・生産プロセス改革を実現したファクトリー実現

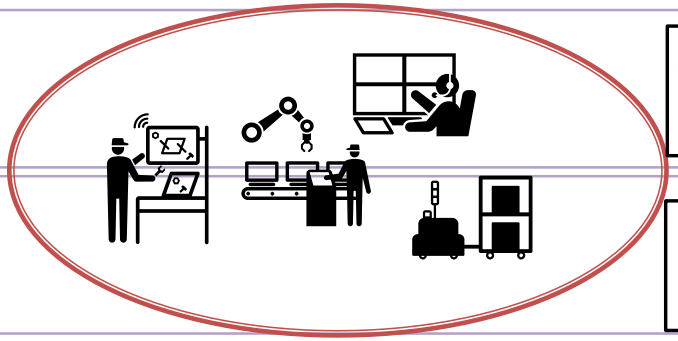
広くつながり＋スマートなファクトリーの実現

エンジニアリングで

業務連携：的確に
業務システム、エンジニアリングシステムとの連携
社外システム（クラウドサービス含む）との連携
業務端末の活用

現場で

高機能化：より高度に
機器をリアルタイム性高く制御し動かす
高度な機器を導入



インテリジェント化：賢く
AIで考え賢く自動化・最適化

機器連携：連携し効率よく
メーカと世代の壁を越えて
製造現場の様々な機器を迅速に接続

	分類	システムへの要求	システムの変化
現場で	基盤	市場、ビジネス変化による製品やサービスのライフサイクル短期化と同期した、生産ラインや制御システムの短期間での構築	流通ハードウェア、流通ソフトウェア（市販パッケージ、OSS）、高機能装置の活用
エンジニアリングで	機能（現行改善）	高効率を目指し、社内外のデータ、機能の活用（受注、CAD、データ解析、リモート保守など）	クラウドサービスを含む社内外の業務関連システムと連携（受注、CAD、データ解析、リモート保守など）
	機能（新規展開）	より高度な制御やサービスを目指し、Society5.0（CPSF）での新たな業務機能構築	サイバー空間レベルでの価値創造によるスマート化（高機能、品質）

工場のスマート化に伴うリスクを管理していくための考え方の仮説

- 工場のスマート化を進めていくためには、付随するリスクを管理するための考え方や対応のあり方を検討する必要性が生じていると考えられる。
- 具体的には、汎用品活用への対応、外部連携対応、新たな制御モデルへの対応について検討が必要であるとともに、スマートファクトリーに対応できる人材のあり方について、検討を進めていくことが必要と考えられる。
- また、汎用品の活用や連携の増加に伴い、サプライチェーンで考慮しなければいけない事項も変化・増加し得ることから、スマートファクトリー特有のサプライチェーン対応についても、検討を進めていくことが必要と考えられる。
- 加えて、戦略的イノベーション創造プログラム（SIP）においてもスマート工場のセキュリティに資する技術開発がなされていることから、こうした技術との連携も模索していくことが効果的と考えられる。

分類	従来のセキュリティ施策の考え方	スマートシステム化に伴うセキュリティ施策へのインパクト
基盤	・ホワイトボックスの考え方で構築 ・制御システムをシェル化（シェルの核ほどホワイトボックス）し、シェルの境界でシステム、運用にてセキュリティ施策を実施。	流通品の活用によりシェル内の各所でブラックボックスの汎用品を活用するため、既存の考え方（シェルの界面でガード）でのセキュリティ施策が有効でなくなる。 →・シェル内のブラックボックスの汎用品からインシデントが発生
機能（現行改善）	・制御システム機能と連携システムの機能と直接の連携はない（停止しても制御への直接影響しない） ・連携するデータは独自形式 ・制御システム機能のセキュリティは各機能が独自に実施。	制御機能の一部として社内外システムの機能を利用 社外システムとのデータ交換も中心に標準データ形式を利用 →・外部システムでのセキュリティインシデントによる不正データが制御に影響 ・標準的なプロトコルを利用するマルウェアの影響を受けるためインシデント発生可能性が拡大
機能（新規展開）	・確立された制御ロジックをベースに制御システムの機能を実現。このためロジックが正しく実装されているかを検証する構築段階での施策によりセキュリティを実現。	サイバー空間にフィジカルの世界をモデル化し高度な制御システムの機能を実現するという新たな制御モデルの誕生。 →新しい考え方のためセキュリティリスク分析およびセキュリティ施策が不明 ・誤ったモデル実装によるインシデント発生 （モデルの誤った利用によるインシデント発生モデルの改ざんを含む）

システム/運用/マネージメント

汎用品活用（ゼロトラスト範囲拡大）への対応
- ハードウェア　・ソフトウェア
- 機能　・サービス

外部連携対応
- 標準データ活用時のセキュリティ施策
- 不正データに対応するセキュリティ施策（CPSF2層の対応）

新たな制御モデルへの対応
- 装置、機能動作モデル化時のセキュリティ施策
- モデル利用時におけるセキュリティ施策（CPSF3層の対応）

人材

スマートファクトリー対応スキル向上
- 変化に対応できる知識
- 多様なインシデントの経験

サプライチェーン

外部連携に係る契約先との留意事項

OSS等の開発プロセスでの留意事項

クラウド等の調達・契約の留意事項

スマートファクトリーガイドを通じ、先進的な事業者が臆することなく工場のスマート化を進め、「稼げる工場化」を促進することを後押ししていく。

「工場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」拡充版

- 工場のスマート化において検討すべきセキュリティについて、昨年度公表した「工場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」拡充版として整備する。
- 「工場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」に記載した実施事項（ステップ1・2・3）と整合を取り、各ステップにおいてスマート化の際に留意すべき点や対策のポイント等について、別冊で整理する。

「工場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」本編　目次

1. はじめに
2. 本ガイドラインの想定工場
3. セキュリティ対策企画・導入の進め方
3.1 ステップ1
内外要件（経営層の取組や法令等）や業務、保護対象等の整理
3.2 ステップ2
セキュリティ対策の立案
3.3 ステップ3
セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

付録A 用語／略語
付録B 工場システムを取り巻く社会的セキュリティ要件
付録C 関係文書におけるセキュリティ対策レベルの考え方
付録D 関連／参考資料
付録E チェックリスト
付録F 調達仕様書テンプレート（記載例）

目次構成を整合

「工場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」拡充版　目次（案）

1. はじめに
2. 本ドキュメントのスマート工場
3. セキュリティ対策企画・導入におけるスマート化のポイント
3.1 ステップ1
内外要件（経営層の取組や法令等）や業務、保護対象等の整理
3.2 ステップ2
セキュリティ対策の立案
3.3 ステップ3
セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

本編の基本的な実施事項を確認しながら、拡充版でスマート化のポイントを参照可能とする。

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html