資料5

令和2年度
スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査

結果概要

三菱総合研究所

デジタル・イノベーション本部
サイバーセキュリティ戦略グループ

2021年12月

調査の背景・目的

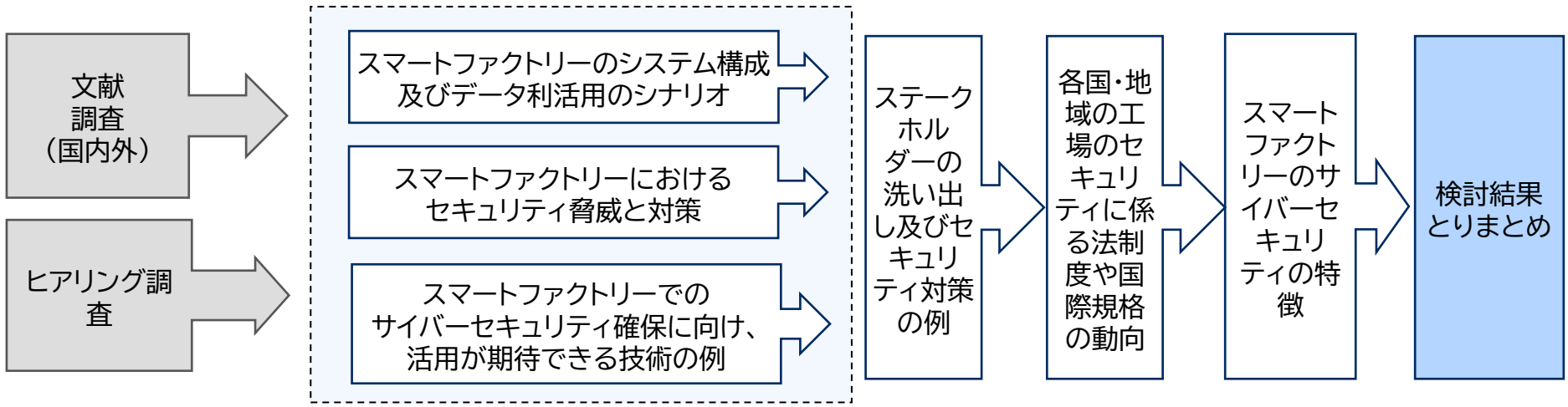
【背景】

- 工場分野の制御システムは、内部ネットワークとして、インターネットには曝されないことを前提に設計されてきた。他方、IoT化や自動化の流れの中でスマートファクトリーへの注目が高まり、個別の機械やデバイスの稼働データを取るために、末端の機器がネットワークにつながることとなり、新たなセキュリティ上のリスク源になり得る。そのため、サイバーセキュリティ対策について特別な対応が求められると考えられる。

【目的】

- 本事業では、製造現場でのサイバーセキュリティ対策を検討するために、国内外の工場セキュリティ対策の動向について調査を行うとともに、工場に必要なサイバーセキュリティ対策を実際に実施していくために有用なガイドラインの策定に向け、国内の企業や業界団体、有識者にヒアリングを行い、その結果をとりまとめることを目的とする。

調査フロー



スマートファクトリーの段階

- ドイツの「インダストリー4.0 実現戦略」では、インダストリー4.0は「製品のライフサイクルを通じて価値連鎖全体の組織と制御が新たなる段階に入ることを意味する。このサイクルは個別化の進む顧客の要望に対応するもので、アイデア段階から開発および製造の指示、製品の末端顧客への納品、果てはリサイクリングまですべての段階を指し、それに関連するサービスも含む。」とされている。
- しかし、「インダストリー4.0」はまだ実現されておらず、特に日本においては多くの製造業においてようやくデータの利活用が始まりつつある状況である。スマートファクトリーのセキュリティを検討するにあたり、将来的に目指す姿を念頭に置くことは重要であるが、データの利活用を開始したばかりの工場から、ある程度活用が進む工場まで考慮する必要がある。
- そこで、データの活用度合いに応じて、複数の段階があることを想定した上で、スマートファクトリーのセキュリティを検討した。

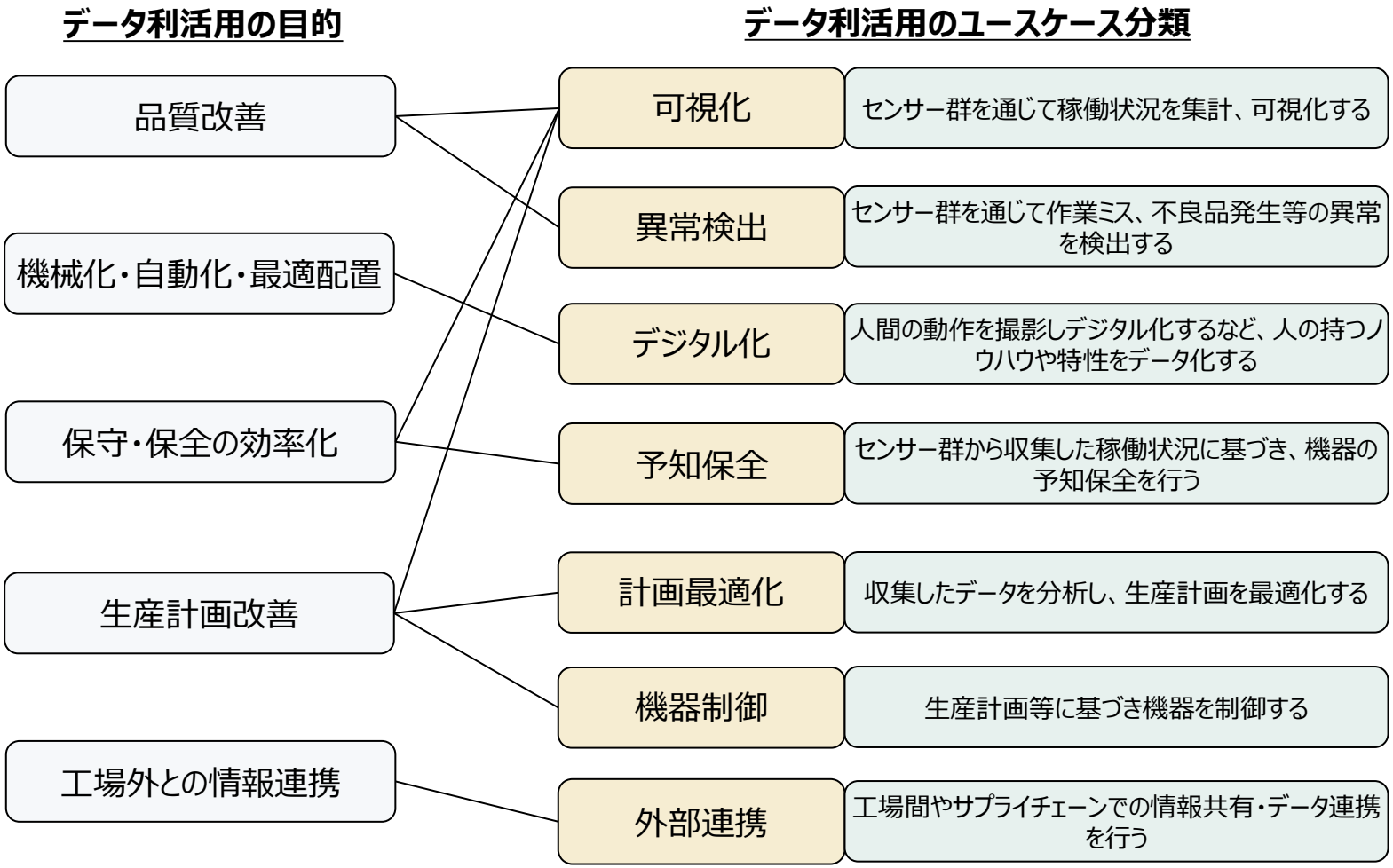
スマートファクトリーの段階

レベル0	レベル1	レベル2	レベル3	レベル4
従来の工場	データの収集・蓄積	データによる分析・予測	データによる制御・最適化	動的な自律制御
情報がまだ活用されていない。	有益な情報を見極めて収集して状態を見える化し、得られた気付きを知見・ノウハウとして蓄積できる。	膨大な情報を分析・学習し、目的に寄与する因子の抽出や、事象のモデル化・将来予測ができる。	蓄積した知見・ノウハウや、構築したモデルによる将来予測を基に最適な判断・実行ができる。	複数の工場または事業者が接続し、解析結果や予測を基に、各主体が自律的かつ動的に制御できる。
従来の工場	スマートファクトリー			

資料：経済産業省中部経済産業局「スマートファクトリーロードマップ」（2017年5月）を基に作成

データ利活用事例のユースケース分類

- スマートファクトリーの事例を調査し、スマートファクトリーにおけるデータ利活用の目的と、それぞれの目的に対応するユースケースを以下の7種類に分類した。



データ分類

- 利活用されるデータについて、一次データ及び各種の加工データを以下の８種類に分類した。

利活用データ分類	略称	データ概要	典型的なデータの流れ
センサーデータ	センサー	機器や組立等のリアルタイムの状態を各種センサーを用いて取得したデータ。	フィールド内のセンサーで取得され、フィールド系NW、制御系NWまたはそれ以外のネットワーク経路を通じて情報系NWやクラウド等に送られる。
静止画データ	静止画	機器や組立等の状況を静止画で取得したデータ。	フィールド内のカメラで撮影され、フィールド系NW、制御系NW以外のネットワーク経路あるいは記憶媒体を通じて情報系NWやクラウド等に送られる。
動画データ	動画	機器や組立等の状況を動画で取得したデータ。	フィールド内のビデオカメラで撮影され、フィールド系NW、制御系NW以外のネットワーク経路あるいは記憶媒体を通じて情報系NWやクラウド等に送られる。
制御コマンド	制御CMD	制御の状態を変更するために、送られる命令や指示値。	HMIから入力され、またはMESからゲートウェイを通じてPLC等のコントローラに送られる。
エンジニアリング設定	ENG設定	制御のためのレシピ等各種の制御値を調整するためのプログラムやデータ。	EWSで作成され、PLC等のコントローラに送られる。
機器状態値	機器状態	機器や組立等のリアルタイムの内部状態を表すデータ。	フィールド内の機器で生成され、インターネットや専用線等を通じて保守サービスプロバイダ等に送られる。
生産計画値	生産計画	生産計画を表す日程、生産能力、在庫等の諸データ。	MESで作成され、保持される。
集計分析データ	集計分析	収集したデータを人間が理解しやすいよう集計・加工・分析・可視化するなどしたもの。	制御情報系NW、情報系NW、クラウド等で生成され、各種端末で参照される。

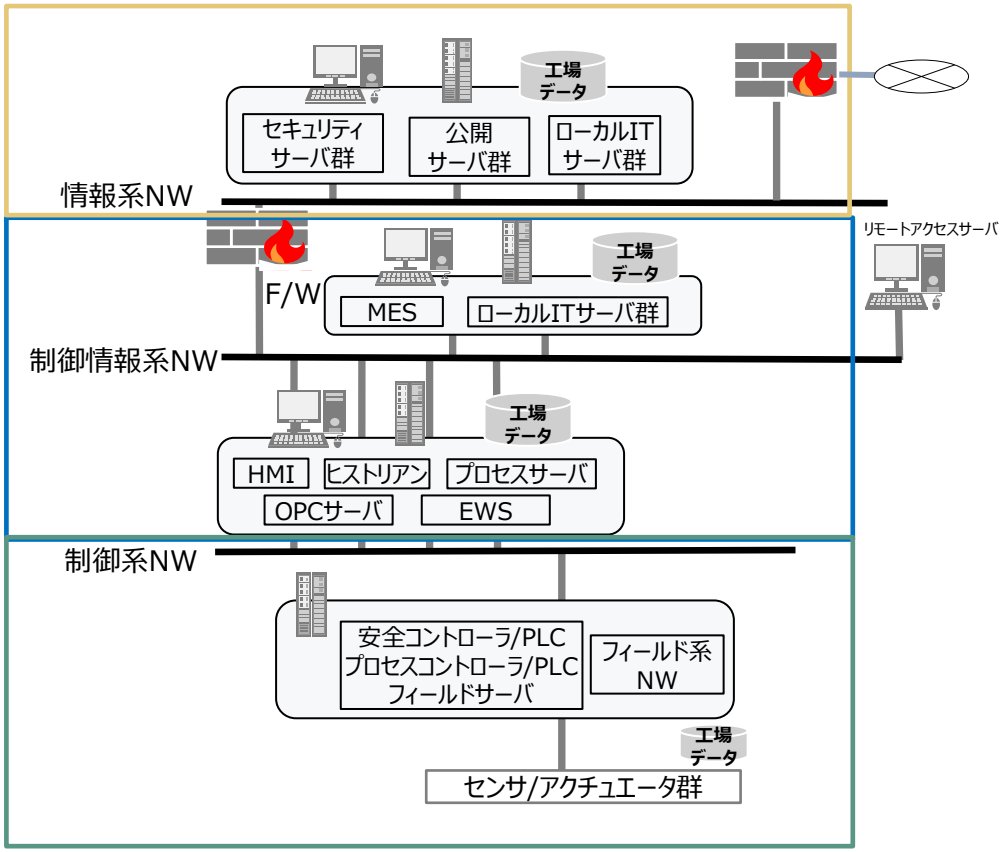
データ毎のリスク

- 利活用されるデータ分類ごとに、データの窃取や改ざん等に伴うリスクを検討した。
- 画像データについては、フィールド内の機器や組立等の機密が視覚的に漏洩するため、データを窃取されたときのリスクが比較的高いと考えられる。
- 制御コマンドやエンジニアリング設定については、機器の正常な動作に支障をきたし可用性に影響を及ぼすおそれがあるため、データを改ざんされたときのリスクが比較的高いと考えられる。
- 集計分析データ等についても、データの性質等によっては機密性がありリスクが高くなる場合もあり得る。

データ分類	データの窃取・改ざん等のリスク
センサーデータ	部分的な窃取ではフィールド内からの具体的な機密漏洩に至る可能性は低い。改ざんされた場合、情報が撹乱されるリスクはあるが、正常稼働に直接影響するおそれは少ない。
静止画データ	**窃取された場合、フィールド内の機器や組立等の機密が（静止画情報という形で）漏洩する。**
動画データ	**窃取された場合、フィールド内の機器や組立等の機密が（動画情報という形で）漏洩する。**
制御コマンド	**改ざんされた場合、誤った制御情報により正常稼働できなくあるおそれがある。**
エンジニアリング設定	**投入するプログラムへのマルウェア混入等により正常稼働できなくあるおそれがある。**
機器状態値	部分的な窃取ではフィールド内からの具体的な機密漏洩に至る可能性は低いため、リスクは比較的低い。
生産計画値	窃取された場合、生産計画という内部情報が漏洩するおそれがある。改ざんされた場合、情報の解釈を誤るおそれがある。
集計分析データ	窃取された場合、（情報処理後の）非公開情報が漏洩するおそれがある。改ざんされた場合、情報の解釈を誤るおそれがある。

スマートファクトリーにおける主なシステムモデルの設定

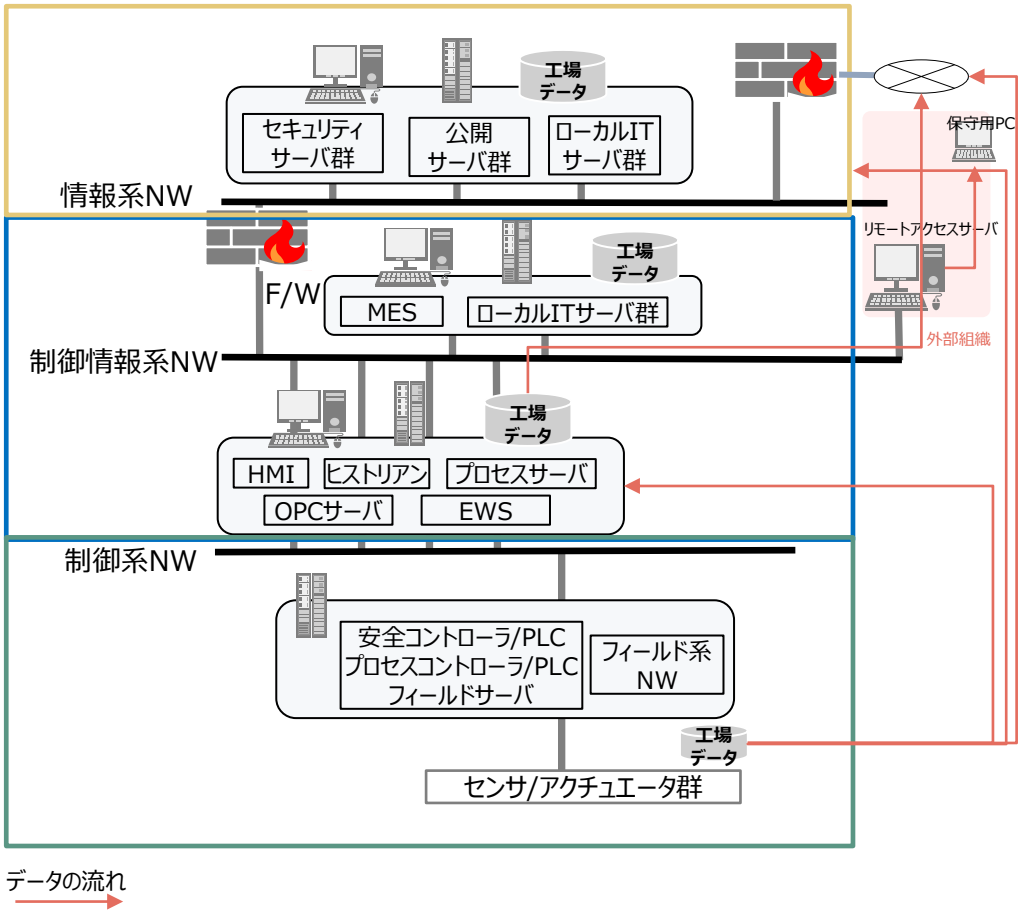
- スマートファクトリーの事例調査結果を踏まえて、スマートファクトリーにおける主なシステムモデルを設定した。
- データの接続に着目した場合、「制御系NWデータ（工場内部データ）」「制御情報系NWデータ」「情報系NWデータ」が、それぞれ従来のクローズな工場システムでは接続していなかった、新たな接続先に接続することによるシステムモデルが設定できる。
- データ分析に着目した場合、データ分析が「制御情報系NW」「情報系NW」に接続された機器、または「外部」のどこで分析されるかという観点でシステムモデルが設定できる。
- 制御システムに対するアクセスに着目した場合、コントローラ/PLCに接続する「制御情報系NW」のEWS等にインターネットで接続するモデルが設定できる。



※ 経済産業省・NEDO・三菱総合研究所「IoTセキュリティ対応マニュアル産業保安版（第2版）」を基にMRI作成

スマートファクトリーにおける主なシステムモデルの設定
（1）工場内部データの工場内外への接続

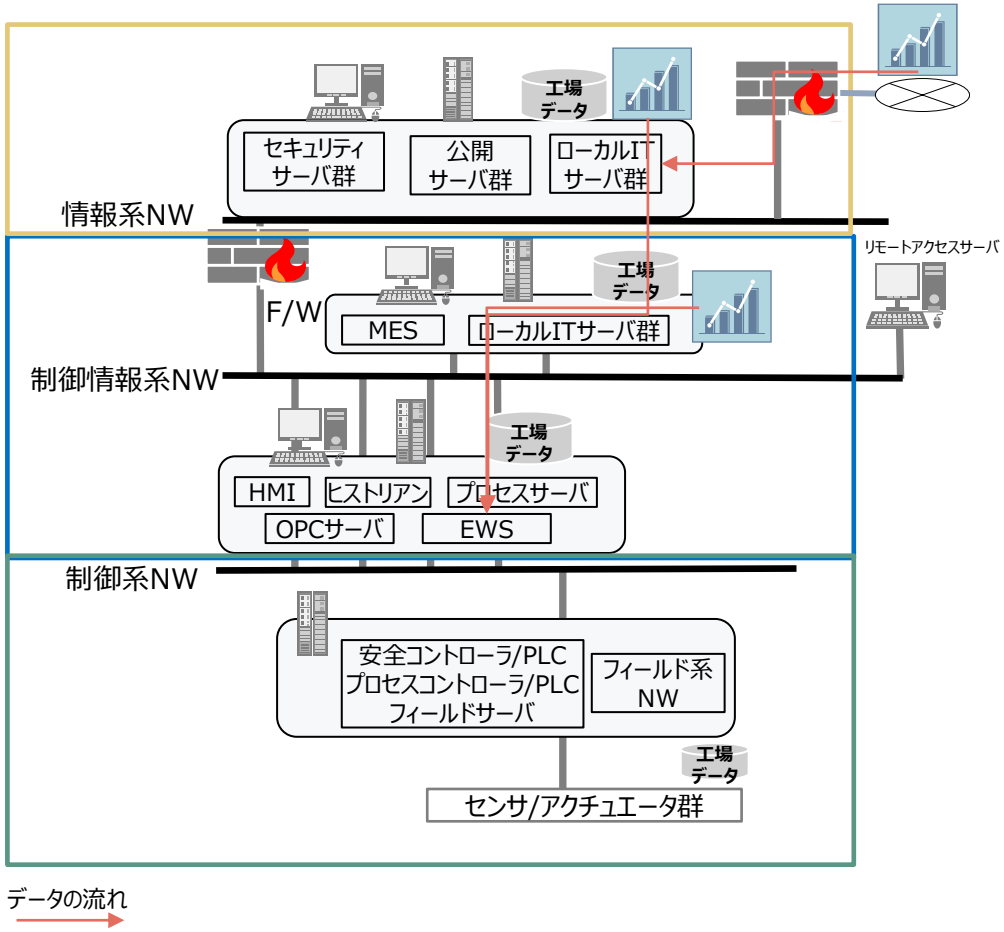
- データの接続に着目した場合、スマートファクトリーの場合は、特に工場現場にある「制御系NWデータ（工場内部データ）」の活用が進んでいる。
- 従来の工場では「制御系NW」「制御情報系NW」「情報系NW」が三層に分かれていたが、無線通信などにより、これらのネットワーク接続以外の経路により工場データが送受信される場合がある。
- 従来はそれぞれの境界で守ることができたが、このような接続の場合、ネットワーク境界だけで守るだけではなく、新たな接続点や接続回線におけるセキュリティ等に留意が必要となる。



※ 経済産業省・NEDO・三菱総合研究所
「IoTセキュリティ対応マニュアル産業保安版（第2版）」を基にMRI作成

スマートファクトリーにおける主なシステムモデルの設定
（2）集計分析データの工場における活用

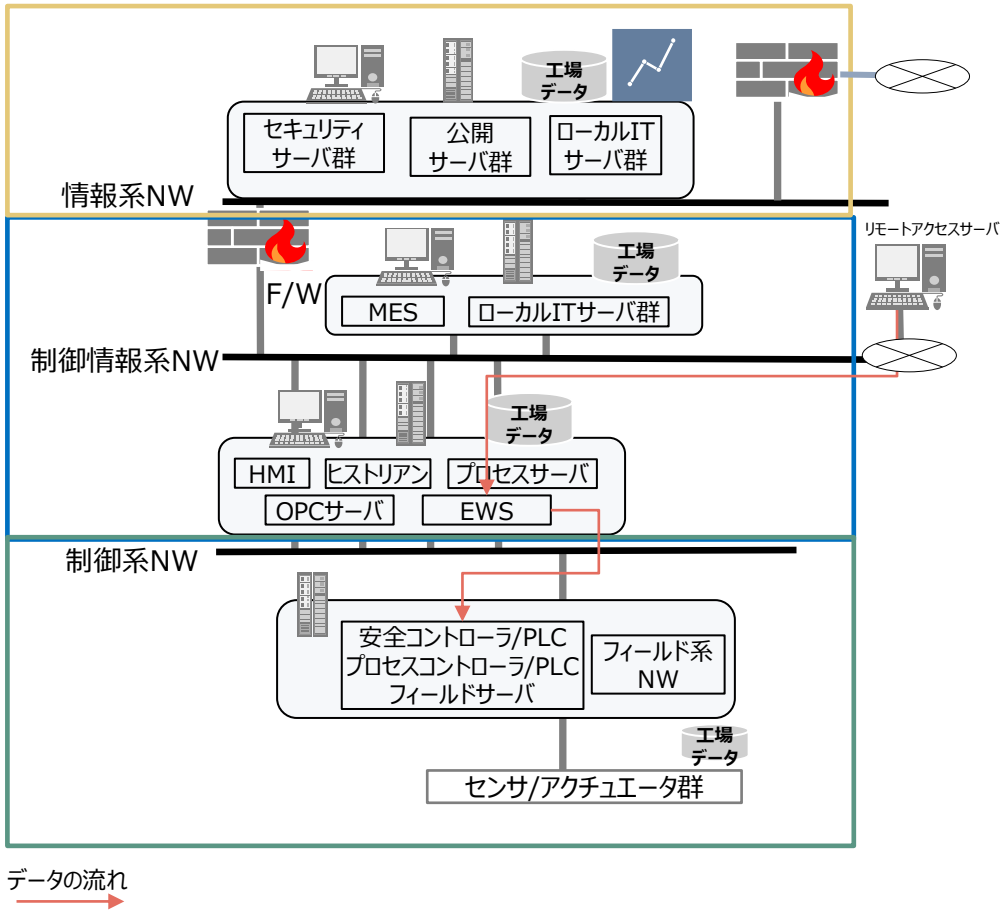
- データ分析に着目した場合、データ分析が「制御情報系NW」「情報系NW」に接続された機器、または「外部」のどこで分析されるかという観点でシステムモデルが設定できる。
- データ分析において外部を利用する場合は、外部接続及び外部保存（クラウド）のセキュリティに留意が必要である。AI等の技術が用いられる場合、分析を行う機器において正しい分析がなされるか、制御に関係するデータが正しいか等のセキュリティ等に留意が必要となる。（ただし、リアルタイムかつ自動で制御を行うケースは見られない）



※ 経済産業省・NEDO・三菱総合研究所
「IoTセキュリティ対応マニュアル産業保安版（第2版）」を基にMRI作成

スマートファクトリーにおける主なシステムモデルの設定
(3)リモートメンテナンス

- 制御システムに対するアクセスに着目した場合、コントローラ/PLCに接続する「制御情報系NW」のEWS等に、リモートメンテナンスのために外部から接続するモデルが設定できる。
- リモートメンテナンスの接続先、リモートメンテナンス回線のセキュリティ等に配慮が必要となる。



※ 経済産業省・NEDO・三菱総合研究所
「IoTセキュリティ対応マニュアル産業保安版(第2版)」を基にMRI作成

想定される脅威と必要なセキュリティ対策例

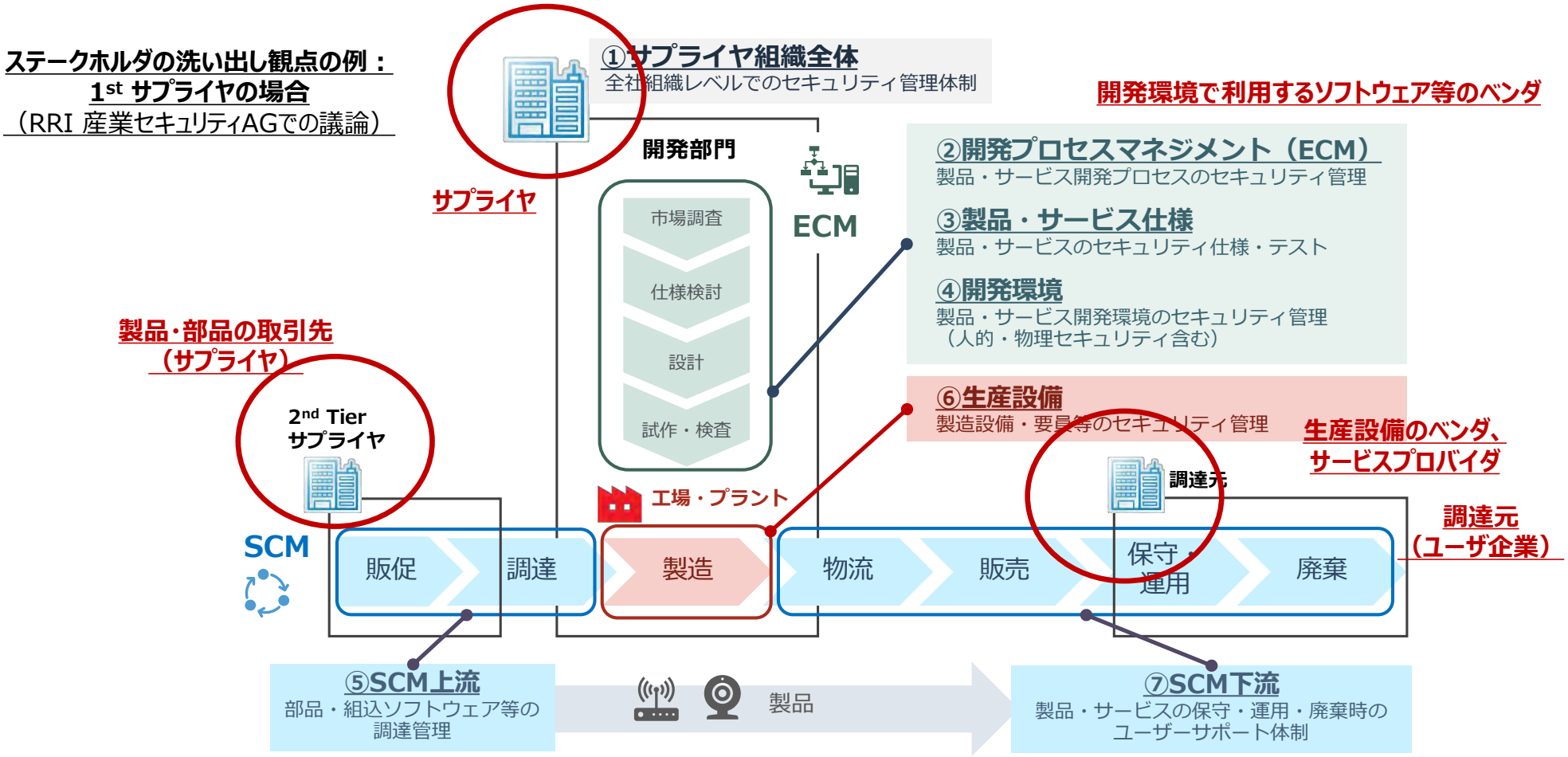
- システムモデルにおいて想定される脅威と必要なセキュリティ対策例を整理した。

脅威とセキュリティ対策（例）

	想定される脅威	必要なセキュリティ対策（例）
工場内部データの工場内外への送信	• データを送受信するネットワークへの不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等 • データを集約する機器への不正アクセスに基づくデータ改ざん、データ窃取等 • クラウドに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等 • 外部事業者のなりすましによるデータ改ざん、データ窃取等	• ネットワークへの不正侵入防止 • 機器の認証 • リモートアクセスサーバや保守用PCの不正侵入防止 • 無線通信の認証、暗号化 • セキュリティが確保されたクラウドサービスの利用 • 接続先（人）の認証 • データの妥当性検証
集計分析データの工場における利用	• 情報系ネットワークに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等 • クラウドに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等 • 外部事業者のなりすましによるデータ改ざん、データ窃取等	• ネットワークへの不正侵入防止 • セキュリティが確保されたクラウドサービスの利用 • 接続先（人）の認証 • データの妥当性検証 • 分析の妥当性検証
リモートメンテナンス	• 外部ネットワークに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等 • 外部事業者のなりすましによるデータ改ざん、データ窃取等	• ネットワークへの不正侵入防止 • セキュリティが確保されたクラウドサービスの利用 • 接続先（人）の認証 • データの妥当性検証
全般	• デジタルデータ化・蓄積・集計等を行う各種サーバ（ITサーバ）のマルウェア感染 • MESのマルウェア感染 • EWSのマルウェア感染 • OPCサーバーのマルウェア感染 • 入力・表示するモバイル端末のマルウェア感染	• 各種機器のマルウェア対策 • データの妥当性検証 • セキュリティを考慮した標準規格への準拠 • 各種機器の脆弱性管理

ステークホルダーの洗い出し

- ステークホルダの洗い出しに際しては、工場におけるサプライチェーンのセキュリティ対策要件を検討中のRRI産業セキュリティAGでの議論を元に、サプライチェーンマネジメント及びエンジニアリングチェーンマネジメントの両面から洗い出した。



主なステークホルダー

スマートファクトリーに関わる主なステークホルダー

	ステークホルダー	内容
1	ユーザー企業	スマートファクトリーのセキュリティ確保において最も重要な役割を果たすのが、ユーザー企業である。セキュリティを推進する主体となり、セキュリティ要件の策定や予算の確保等を行う役割を果たす。ユーザー企業の中でも、経営者、IT部門、OT部門（生産技術等）等、役職や部門によりそれぞれの役割は異なる。
2	部品・製品サプライヤー	スマートファクトリーにおいて製造される製品のセキュリティ確保のためには、その製品を構成する部品や製品のサプライヤーも、部品・製品のセキュリティ確保が求められる。そのため、部品や製品のサプライヤーは重要な役割を果たす。部品や製品の性質や納品先との契約によっては、納品後の利用・運用時においても、脆弱性管理などのセキュリティ面でのサポートが求められる。
3	生産設備のサプライヤー	スマートファクトリーの工場システムを構成する生産設備に対してもセキュリティ確保が求められることから、生産設備のサプライヤーも重要な役割を果たす。生産設備自体がスマート化することで、機器そのものにおいて必要なセキュリティ要件を備えていく必要がある。また、生産設備においても利用・運用時において、脆弱性管理などのセキュリティ面でのサポートが求められる。
4	システムインテグレーター、販売会社	スマートファクトリーの工場システムを構成する生産設備や各種機器においては、単体でのセキュリティ確保は必要であるものの、最終的に複数の機器を接続してシステムとして納めるシステムインテグレーターや販売会社等の果たす役割も大きい。ユーザー企業とのニーズや要件を把握できる立場にあり、システム全体としてのセキュリティを検討し、実装する役割を果たす。
5	製品開発環境ソフトウェア等ベンダー	製品のセキュリティを確保するためには、製品開発環境のセキュリティも必要となる。そのため、製品開発環境において利用されるソフトウェア等を提供するベンダーが関わる。
6	ネットワークベンダー、クラウドベンダー	スマートファクトリーにおいて、情報系ネットワークとの接続や外部との接続が増えることでネットワークベンダーの関わりが増えてくる。工場システムでのセキュリティ対策が難しい場合、ネットワークセキュリティの確保が果たす役割も大きくなる。ネットワークベンダーには、今後ローカル5Gの提供事業者も加わることが想定される。 また、スマートファクトリーによってクラウドサービスの利用が増えることから、クラウドベンダーの関わりが重要となる。
7	セキュリティベンダー	スマートファクトリーにおいてもセキュリティベンダーが提供する製品・サービスが活用されることから、セキュリティベンダーが関わる。制御システム向けのセキュリティを提供するベンダーも増えつつある。
8	利用時の関連事業者	製品・サービスの利用時には、物流事業者、販売・構築の部分でシステムインテグレーターや販売会社、部品提供者、保守・運用事業者、廃棄事業者と別々の事業者が関わる。

ヒアリング結果　まとめ①

ガイドラインの対象

- スマートファクトリーにおいては、ユーザー企業（工場）が製造する製品にもバリエーションがあり、ステークホルダーも多様である。ガイドラインについては、想定読者と目的を明確にすべきであるという意見が得られた。対象とする工場を考える上でのポイントを以下に整理する。

＜新設・既設＞

- 工場の新設・既設により取り得る対策は異なる。
- また、新設の工場であっても、既設工場から古い設備を移動して利用するケースもある。
- 古い設備の場合は、レガシー機器のセキュリティ対策についての考慮が必要である。
- 繋げた結果、ネットワークセキュリティが不完全だったり、プログラムに脆弱性のある古い端末が接続されていたりする。
- 運用の手間を考慮すると、古い設備を活かすのがよいのか、作り替えるのがよいのか、セキュリティを考慮したコスト効果を考えてもよい。

＜規模＞

- 工場は大半が中小規模であり、どう巻き込んで対策を推進していくかが課題である。

＜データ活用の進展度＞

- データ活用や接続等のグレードに応じたスマートファクトリーの類型化があれば、この類型のスマートファクトリーはこのくらいのセキュリティが必要、といった整理ができるのではないか。類型化だけでも参照する価値のあるガイドラインになると考えられる。

＜リスク＞

- リスクによって取り得るセキュリティ対策は異なることから、同じような脅威、リスクが想定されるメンバーにより検討を進めてはどうか。

ヒアリング結果　まとめ②

対応すべきリスク

- 基本的な考え方としては、リスクベースで検討した上でセキュリティガイドラインをまとめるべき、という意見であった。
  - セキュリティの議論はリスクベースとする必要がある、
  - セキュリティリスクはユースケースで議論を深めていく必要がある。そのため、スマートファクトリーで考えられるユースケースはこういうモデルで、リスクはこう考えられ、ステークホルダーは誰、脅威は何、だからこういう対策をすべきのように、シナリオを想定して整理する良い。ライフサイクル毎でもリスクが異なる。
  - どこまでのリスクを許容して、どこからリスク対策を検討するのかの整理が必要である。また、どこまでの攻撃シナリオを想定するかも要検討である。

- リスクに対する対策の考え方としては、海外動向と調和する形で、CPSFとの確認を行いながら整理することが受け入れられやすいと考えられる。
  - 議論を進める上では、国際規格（IEC62443、NIST CSF、NISTIR 8183）等の拠り所があることで、海外規格の整理に対する日本としての対応というストーリーが受け入れられやすいのではないか。
  - 海外の規制（特にEU）や業界毎の規制と整合性の取れたガイドラインとすることが必要である。

- 提供側としては、どこまでのセキュリティが求められるかを提示できると有効と考えられる。
  - システム単位のセキュリティ、製品単位のセキュリティ、部品単位のセキュリティと考えられるが、部品に対してどこまでのセキュリティについて求められるかを示してほしい。
  - 例）センサーというフィジカルからサイバーに切り出す部分で、どこまでセキュリティを考えるべきか。バックドアをしかけられていないか、製品として正しく作られているかどうかを証明する必要があるのではないか。運用時に一部の部品を入れ替えるときに、それが本物であることの証明が必要かもしれない。

ヒアリング結果　まとめ③

対策を進める主体

スマートファクトリーのステークホルダーは様々であり、各々がセキュリティについて実施すべきことを進める必要がある。各ステークホルダーが対策を推進する必要性等について以下に整理する。

ユーザー企業（工場）：

エンドユーザーがセキュリティ対策の必要性を認識し、予算を確保することが最も重要である。予算がなく、仕様としてセキュリティが示されない限り、提供側からセキュリティを強化する提案にはならない。また、工場内に複数のラインが存在し、様々なベンダーのシステムや機器が混在することから、システムの全体像を把握できるのはユーザー企業側のみとなる。工場側の設備について所管する生産技術部門の方々の意識を高め、セキュリティ対策を推進することが必要である。また、ユーザー企業側には、セキュリティ対策を推進する人材と、現場で実際に対策検討・導入・運用・評価する人材のいずれもが必要となる。

ユーザー企業（工場・中小規模）：

中小企業向けのセキュリティ対策を進めることが、サプライチェーン全体のセキュリティ確保に重要である。中小企業向けにガイドに記載する内容としては、啓発的な内容で、導入のしやすさやセキュリティがわからなくても容易にできる取り組みが求められる。

工作機器メーカー：

欧米の工作機械メーカーがIEC62443-4-2認証を取得する動向が見られた。工作機器メーカーの委託先への要求も想定されることから、委託先も含めて、工作機器メーカーに対して、欧米の規格に沿った形で対策を提示することは、工作機器におけるセキュリティ対策を推進する上で有効と考えられる。メーカー社内において、製品セキュリティを主管する部門が存在しない場合もあり、また、製品は企画・設計～開発～製造～運用～廃棄までライフサイクルがあるため、各ライフサイクルにおいてどの組織がどう対応するのか、全体のセキュリティをどう確認するか等、社内体制も考慮する必要がある。

システムインテグレーター、販売会社：

工作機器メーカーやPLCメーカーにとって自社製品のセキュリティ確保は重要であるが、ユーザー企業の環境や要件に合わせてシステムとして納めるシステムインテグレーターや販売会社が、システムとしての全体的なセキュリティ評価を行い、適切な箇所にセキュリティ対策を施して、納入できることは重要である。外部に接続しないことを前提とした古い設備が工場に残ることも多く、クラウドに繋ぐとことで問題が発生するリスクもある。

ネットワークベンダー、セキュリティベンダ

ユーザ企業におけるデータ活用が限定的（OA系のPCを通るのみ等）であれば、ネットワークセキュリティにより一定レベルの対策が可能となる。また、ユーザー企業において工場側の担当がセキュリティについて詳しくない場合、ネットワークに接続するタイミングの検討でIT側の担当者からセキュリティが求められる場合がある。その際に、ネットワークベンダーとして適切にセキュリティ対策を提案できることは重要である。将来的にローカル5Gの提供事業者が加わった場合の安全性についても考慮が必要である。