インダストリー4.0実現戦略
プラットフォーム・インダストリー4.0
調査報告
Umsetzungsstrategie Industrie 4.0
Ergebnisbericht der
Plattform Industrie 4.0
(翻訳版)

全文翻訳 Vollständige Übersetzung

原語：ドイツ語 Ausgangssprache: Deutsch

原版発行：2015年4月ベルリン

Original erschienen: April 2015, Berlin

翻訳：ドイツ国家検定公認通訳・翻訳士　井上　英巳

Übersetzung: Hidemi Inoue, allgemein beeidigt u. öffentlich bestellt.

2015年8月

日本貿易振興機構（ジェトロ）
ベルリン事務所
海外調査部　欧州ロシアCIS課

ドイツ IT・通信・ニューメディア産業連合会(BITKOM)、ドイツ機械工業連盟(VDMA)、ドイツ電気・電子工業連盟(ZVEI)の 3 業界団体は 2013 年 4 月、ドイツ連邦政府の Industrie4.0 構想を受け、その具体化・実現化に向けた「インダストリー4.0 プラットフォーム」事務局を立ち上げた。

同事務局は、発足以来、8 優先分野の研究開発ロードマップの作成など精力的に作業、提言行ってきたが、産業界だけでは同構想の実現に必要な、幅広い課題への対応に限界が生じつつあった。このため、2015 年 4 月のハノーバー・メッセの開催に合わせて、政府、産業界、労働組合や研究所が参加する裾野の広いプロジェクトへと発展的に解消し、新たな「インダストリー4.0 プラットフォーム」事務局に再編された。同プラットフォームには、ドイツ経済エネルギー省や教育研究省などが参加している。

新たなインダストリー4.0 プラットフォーム事務局は、インダストリー4.0 のさらなる実現のために、ドイツ産業界や各種団体の協力を得て「インダストリー4.0 実現戦略」をまとめた。

ジェトロは、インダストリー4.0 プラットフォーム事務局の許可を得た上で、「インダストリー4.0 実現戦略」を専門家の協力のもと、原文に忠実に、かつ、読者に分かりやすく翻訳した。

ドイツのインダストリー4.0 の最新動向を紹介する。

アンケート返送先　　FAX：　03-3582-5309
e-mail：ORD@jetro.go.jp
日本貿易振興機構　海外調査部　欧州ロシア CIS 課宛

JETRO

● ジェトロアンケート ●

調査タイトル：インダストリー4.0 実現戦略

今般、ジェトロでは、標記調査を実施いたしました。報告書をお読みになった感想について、是非アンケートにご協力をお願い致します。今後の調査テーマ選定などの参考にさせていただきます。

■質問１：今回、本報告書での内容について、どのように思われましたでしょうか？（〇をひとつ）

４：役に立った　３：まあ役に立った　２：あまり役に立たなかった　１：役に立たなかった

■質問２：①使用用途、②上記のように判断された理由、③その他、本報告書に関するご感想をご記入下さい。

■質問３：今後のジェトロの調査テーマについてご希望等がございましたら、ご記入願います。

■お客様の会社名等をご記入ください。（任意記入）

ご所属	□企業・団体 □個人	会社・団体名
		部署名

※ご提供頂いたお客様の情報については、ジェトロ個人情報保護方針（http://www.jetro.go.jp/privacy/）に基づき、適正に管理運用させていただきます。また、上記のアンケートにご記載いただいた内容については、ジェトロの事業活動の評価及び業務改善、事業フォローアップのために利用いたします。

～ご協力有難うございました～

インダストリー4.0実現戦略

プラットフォーム・インダストリー4.0調査報告

2015年4月

刊記

プラットフォーム・インダストリー4.0（2013〜2015）は
BITKOM（社）・VDMA（社）・ZVEI（社）による共同プロジェクトです。

共同発行人

BITKOM（社）
ドイツIT・通信・ニューメディア産業連合会（社）
Albrechtstraße 10
10117 Berlin-Mitte

Tel.:(030)27576-0
bitkom@bitkom.org www.bitkom.org

VDMA（社）
ドイツ機械工業連盟（社）
Lyoner Straße 18
60528 Frankfurt am Main

Tel.:069.6603-0
zvei@zvei.org www.vdma.org

ZVEI（社）
ドイツ電気電子工業会（社）
Lyoner Straße 9
60528 Frankfurt am Main

Tel.:069.6302-0
kommunikation@vdma.org www.zvei.org

調整・編集・校正

ヴォルフガング・ドルスト，BITKOM（社）

レイアウト・組版

アストリッド・シャイベ，BITKOM（社）

図表

アストリッド・シャイベ，BITKOM（社）

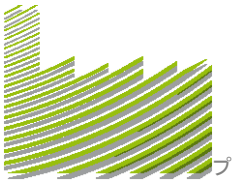
印刷

Kehrberg Druck Produktion Service

写真提供

図17：写真：価値創造の指揮者としての人間：FESTO AG & Co. KG；図22：写真：機械：FESTO AG & Co. KG；写真：ターミナルブロック：PHOENIX CONTACT GmbH & Co. KG；写真：電動軸（左）：FESTO AG & Co. KG；写真：電動軸（右）：FESTO AG & Co. KG；図24および図31：写真：機械1および機械2：FESTO AG & Co. KG；写真：ターミナルブロック：PHOENIX CONTACT GmbH；図25：写真：電動軸（左）：FESTO AG & Co. KG；写真：電動軸（右）：FESTO AG & Co. KG；図26：写真：センサ：Pepperl+Fuchs GmbH；写真：コントローラ：Bosch Rextoth AG；写真：電動軸（左）：FESTO AG & Co. KG；写真：電動軸（右）：FESTO AG & Co. KG；図27：写真：設計：FESTO AG & Co. KG；写真：ハンドブック（左）：FESTO AG & Co. KG；写真：ハンドブック（右）：FESTO AG & Co. KG；写真：電動軸（中段1）：FESTO AG & Co. KG；写真：電動軸（中段2）：FESTO AG & Co. KG；写真：電動軸（中段3）：FESTO AG & Co. KG；写真：電動軸（中段4）：FESTO AG & Co. KG；写真：電動軸（下段1）：Pepperl+Fuchs GmbH；写真：電動軸（下段2）：FESTO AG & Co. KG；図28：写真：機械：FESTO AG & Co. KG；写真：ターミナルブロック：PHOENIX CONTACT GmbH & Co. KG；写真：電動軸（左）：FESTO AG & Co. KG；写真：電動軸（右）：FESTO AG & Co. KG

2015年4月刊行



プラットフォーム

インダストリー4.0

目次

1	まえがき	6
2	インダストリー4.0に関する全般事項	8
2.1	インダストリー4.0の定義	8
2.2	戦略と目標	8
2.3	便益	9
2.4	競合	10
3	学術諮問委員会の命題	12
4	インダストリー4.0実現戦略	15
5	研究と革新	18
5.1	序論	18
5.2	研究項目：価値ネットワークを通じた水平統合	19
5.2.1	新しいビジネスモデル用のメソッド	19
5.2.2	価値ネットワークのフレームワーク	20
5.2.3	価値ネットワークの自動化	21
5.3	研究項目：ライフサイクル全体を通じて終始一貫したエンジニアリング	23
5.3.1	現実と仮想の世界の統合	23
5.3.2	システムエンジニアリング	25
5.4	研究項目：垂直統合とネットワーキングされた生産システム	26
5.4.1	センサネットワーク	26
5.4.2	インテリジェンス－フレキシビリティー変化への対応能力	28
5.5	研究項目：職場環境に配慮した新たな労働インフラ	29
5.5.1	マルチモーダルアシスタンスシステム	29
5.5.2	技術の受容と労働形態	31
5.6	研究項目：インダストリー4.0用の分野横断的技術	32
5.6.1	インダストリー4.0の各種シナリオ用ネットワーク通信	32

5.6.2 マイクロ電子工学 34

5.6.3 セーフティ＆セキュリティ 35

5.6.4 データ解析 36

5.6.5 インダストリー4.0用のシンタックスとセマンティックス 37

5.7 研究項目の相互依存関係と相関関係 38

6 リファレンスアーキテクチャ・標準化・規格化 40

6.1 序論 40

6.2 インダストリー4.0リファレンスアーキテクチャモデル（RAMI4.0） 41

6.2.1 要求条件と目標 41

6.2.2 リファレンスアーキテクチャモデルの簡単な説明 42

6.2.3 リファレンスアーキテクチャモデルの層（レイヤー） 43

6.2.4 ライフサイクルと価値連鎖（Life Cycle & Value Stream） 45

6.2.5 階層レベル（Hierarchy Levels） 46

6.3 インダストリー4.0コンポーネントのリファレンスモデル 47

6.3.1 インダストリー4.0に関する議論との位置づけ 47

6.3.2 他の作業部会による関連資料 48

6.3.3 「インダストリー4.0コンポーネント」 50

6.4 標準化および規格化 63

6.4.1 背景

6.4.2 革新の原動力としての標準化と規格化 64

6.4.3 標準化・規格化団体の協力体制 65

6.4.4 結論 68

6.5 研究事項ロードマップ 69

7 ネットワーキングされたシステムの安全性 71

7.1 序論 71

7.2 想定・仮説・必要条件 73

7.3 インダストリー4.0 脅威の構図 76

7.3.1 企業内に存在する価値 77

7.3.2 可用性と信頼性 77

7.3.3 標的としてのセーフティ 78

7.3.4 整合性 78

7.3.5 機密性 79

7.3.6 改ざん（意図的および非意図的） 79

7.3.7 アイデンティティ盗難 80

7.4 インダストリー4.0の安全目標とセキュリティ要求条件 80

7.4.1 全般的安全目標 81

7.4.2 インダストリー4.0用のセキュリティバイデザイン 81

7.4.3 アイデンティティ管理 82

7.4.4 動的設定に対応した価値ネットワーク 82

7.4.5 仮想インスタンス用のセキュリティ 83

7.4.6 予防と対応 83

7.4.7 アウェアネス，職業訓練，社員教育 84

7.4.8 作業性 84

7.4.9 標準および規定 84

7.5 模範的なセキュリティ対策 85

7.5.1 セキュリティアーキテクチャ 85

7.5.2 アイデンティティ管理 87

7.5.3 暗号 – 機密性の保護 88

7.5.4 暗号 – 整合性の保護 88

7.5.5 安全な遠隔アクセスと頻繁な更新 89

7.5.6 プロセスと組織的措置 90

7.5.7 アウェアネス 91

7.5.8 企業全体を網羅 91

7.6 展望と要求事項 92

8 付録 95

8.1 参考文献一覧 95

8.2 インダストリー4.0用語集 95

8.3 執筆チーム

まえがき

1 まえがき

物理世界と仮想世界の境界線は，次第に薄れつつあります。知的なセンサやアクチュエータの技術を搭載した物理オブジェクトのネットワーキングが，モノのインターネットの発達に伴って進行しています。ネットワーキングを通じて価値創造に関与するすべてのインスタンスの関連情報が漏れなくリアルタイムに利用可能となり，そのデータからそれぞれの時点において最善の価値創造フローを導出できるようになることで，産業革命の新たなる段階に突入することになり，これをインダストリー4.0と呼びます。インダストリー4.0が各種のテクノロジーに及ぼす影響は進化的なものですが，既存のビジネスプロセスには革命的な変化をもたらし，新たなビジネスモデルも生まれることになるでしょう。しかしそこで焦点となるのは，開発・製造・物流・サービスという産業の中核をなすプロセスの最適化です。

このインダストリー4.0実現戦略は，（BITKOM・VDMA・ZVEIの三団体により組織された）プラットフォーム・インダストリー4.0が，ドイツ産業界の企業や他の各種団体の協力を得て作成したものです。すなわちこれは，産業国ドイツとその産業の存続を確実にするための戦略です。

インダストリー4.0の主な構成要素については，第4章に解説があります。その内容に基づいて第5章「研究と革新」では研究の必要がある重要事項を導出し，研究ロードマップや要項などの形で記載しました。研究ロードマップは，政治および企業による適切な措置や助成手段（最先端クラスタ，デモ用ラボ，デモ装置，デモ工場など）を通じてインダストリー4.0というテーマを有意義な形でさらに進化させてゆくための有効な手がかりとなります。

インダストリー4.0のリファレンスアーキテクチャモデル（略称RAMI4.0）を第6章に示しました。その中では，インダストリー4.0を構成する要素の構造と機能が定義されています。リファレンスアーキテクチャモデルおよびインダストリー4.0コンポーネントの一部について，それが適切と思われる場合には，既存の該当規格をベースとしています。また，新たな標準規格を作成する必要がある事項についても特定し解説してあります。

物理オブジェクトのネットワーキングが進み，その制御が容易になる一方で，ハッカーや情報機関，スパイなどによる脅威が増大していることから，安全性に対する要求は特に厳しいものとなっています。これに関しては第7章に概要をまとめました。

この実現戦略は，ドイツ産業界や技術指向型の業種，研究，政治などの分野からの読者を対象としたものです。特に経営幹部や専門人材，助言者などをはじめとする，ドイツにおけるインダストリー4.0の将来像に関心を持つ人や，その形成に参加したいという人にご一読いただければ幸いです。

インダストリー4.0に関する全般事項

2　インダストリー4.0に関する全般事項

2.1 インダストリー4.0の定義

インダストリー4.0とは，第四次産業革命を表す言葉であり，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。

その基盤をなすのは，価値創造に関与するすべてのインスタンスがネットワーキングされていることによりすべての関連データがリアルタイムで常に利用可能であることと，そのデータからそれぞれの時点で最適な価値創造フローを導出することができる能力である。人・オブジェクト・システムを結ぶことにより，動的でリアルタイムに最適化され，自己組織型の企業横断的価値ネットワークが成立し，費用や可用性，資源消費量などといったさまざまな基準に従っての最適化ができるようになる。

2.2 戦略と目標

業界団体であるBITKOM・VDMA・ZVEIは，経済・学術研究同盟の活動を継続し，統率のとれた業界横断的な対応を行う目的で，プラットフォーム・インダストリー4.0という共同イニシアチブを立ち上げた。プラットフォーム・インダストリー4.0の最重要課題は，BITKOM・VDMA・ZVEI三団体の手でインダストリー4.0構想を推進し，産業界への浸透を図ることにある。これを通じて工業生産国としてのドイツの存続を確実なものとし，さらに強化することを目指している。

経済・学術研究同盟が2013年4月にまとめたインダストリー4.0に関する最終報告書には，実践に向けた提言[3]が盛り込まれ，研究の必要がある分野を取り上げて解説し，八項目の行動分野が規定されているが，以下に現状分析のため各項目を（便益の側面を加味しつつ）列挙しておく。

1. 標準化，リファレンスアーキテクチャのためのオープンスタンダード
   価値ネットワークを通じた企業横断型ネットワーキング・統合を可能にする
2. 複雑なシステムの確実なコントロール
   作業の自動化やデジタルと現実の世界の統合にモデルを利用
3. 全土を網羅した産業用ブロードバンドインフラ
   インダストリー4.0の要件となるデータ交換の容量・質・速度の確保
4. 安全性
   ここで対象となるのは操業の安全性（英語：セーフティ），個人データの保護（英語：プライバシー），ITの安全性（英語：セキュリティ）
5. 作業組織と作業現場の構成
   インダストリー4.0の各種シナリオにおける計画者および意思決定者としての人間ないし労働者にとってどのような意味をもつのかを明らかにする
6. 職業訓練と社員教育
   職業訓練と社員教育の内容および新たな手法を策定
7. 法的な環境条件
   インダストリー4.0に必要な（できる限り欧州レベルで統一された）法的環境条件の整備（デジタル財の保護，システム間で締結された契約に関する契約法，賠償責任の問題など）を目的とする
8. 資源効率
   良識を持ってあらゆる資源（人的資源・財的資源・材料）を活用することが，これからの工業生産を成功させる要素となる

工業生産体制のインダストリー4.0への転換を成功に導くため，ドイツでは二重戦略を採用している。

- 各種設備の世界市場におけるドイツの主導的な地位を維持するため，従来からのハイテク産業に情報通信技術を徹底して取り込み，知的生産技術の模範的サプライヤとなる。CPSテクノロジーおよびCPS製品の模範市場[1]を新たに構築し供給する必要がある。
- また同時に，効率の良い資源節約型の生産技術によってドイツ国内における生産の魅力と競争力をさらに高めることも重要である。地理的な近さとインターネットを通じたユーザーとメーカーの能動的なつながりにより生まれるドイツ国内企業の競争上のアドバンテージを強化することがその狙いである。ドイツ国内の自動化・プロセス・生産などの技術はいずれもこの戦略の恩恵を被る。
- インダストリー4.0への道は進化的なプロセスである。価値連鎖全体の最適化において実績を上げ，その特殊な条件に対応するためには，既存の基礎技術を改良してゆく必要がある。インターネットサービスによる新たなビジネスモデルには破壊的な性格が伴う。良質の製品ないしサービスがあり，事業を展開する市場における需要が伸びている業績の良い企業は，破壊的な変化に備えた十分な態勢を整えることが望ましい。社内の既存プロセスを改良するという側面と，新たなビジネスモデルの開発という側面のいずれについてもである。

1 実践提言書[3]記載の定義：サイバーフィジカルシステム（CPS） CPSには，センサを用いて直接物理データを掌握し，アクチュエータを使って物理プロセスに作用する，デジタルネットワークにより互いに接続された，世界中で利用可能なデータおよびサービスを利用し，マルチモーダルマンマシンインターフェイスを備えた各種の組み込み式システム，生産・物流・エンジニアリング・調整・管理の各プロセス，インターネットサービスなどが含まれる。
サイバーフィジカルシステムはオープンな社会技術システムであり，さまざまな新種の機能・サービス・特性を可能にする。

2.3 便益

価値連鎖に参加する者にとっての便益は多様である。個別化された顧客の要望に対応する能力が向上し，一点や少数のみの個別生産の収益性が上がる。さまざまな次元でのインターネットを介したビジネスプロセスが臨機応変に形成され，エンジニアリングプロセスの機敏な対応により，弾力化がさらに進んでいる。インダストリー4.0がビッグデータやソーシャルメディア，クラウドコンピューティングなどと相まって提供する情報を利用することで，意思決定の最適化や，設計決定のリスクを早期に回避すること，不具合への柔軟な対応，すべての資源をグローバルレベルで立地横断的に最適化することなどが可能になる。

生産効率は，生産性の向上によっても改善するが，資源（機械・エネルギー等）の利用効率が高まることによっても向上する。

新たな形態の価値創造および雇用によって新しい可能性が生まれ，たとえば川下のサービス，すなわち製品が生産施設から出荷された後に，本来の製品を補完する形でユーザーに提供することのできる各種サービスなどが考えられる。

人口構造の変化を考慮した労働のあり方という面においてもメリットがある。たとえば，身体能力および認知能力の支援などが，インダストリー4.0構想がもたらす決定的な付加価値となる。社員の教育水準が高い知識ベース企業が社員の知識と経験を維持するためには，インダストリー4.0を通じて人材育成のための柔軟かつ多様なキャリアモデルが可能となり，経営幹部のみならず，専門人材のキャリアなども考えられる。ソーシャルメディアにより生産計画および労働時間体制の柔軟性が増す。生産プロセスの稼働率が最適化され，資源利用の効率が上がる。さらに，顧客の要望にも迅速に対応できるようになる。また従業員にとっても，人材投入の計画に自ら関与する可能性が拡がることで，仕事と家庭や余暇との両立がしやすくなる。

インダストリー4.0は高賃金国であるドイツの競争力を強化し，模範的サプライヤとしての企業の地位を確立することを可能にして，ドイツをインダストリー4.0ソリューションの模範市場たらしめるものとなる。

我が国産業界の知識は群を抜いており，それは大手企業のみに留まらず，確固とした基盤を有する中小企業も同様で，業種としてはたとえば工業用自動化技術やIT，工具・機械製造などがあげられる。

2.4 競合

インダストリー4.0構想の実現には，製品のライフタイムを通じ，すべての関係者が企業横断的な通信および協力をリアルタイムで確実に行うことが前提となり，インターネットベースのプラットフォームによってそれを実現しようとするものである。このデジタルプラットフォームが，新たな革新的価値連鎖の基盤をなし，インダストリー4.0の便益をもたらす。

このような企業横断的で確実な「水平」方向の通信・協力プラットフォームについて，競争前段階の領域において共通の定義を策定し，多岐にわたる環境条件やさらなる研究の必要性なども合わせて規定するという課題のために，プラットフォーム・インダストリー4.0というイニシアチブが発足したのである。

しかしこれがすべてではなく，物理世界にそれぞれ対応するバーチャルイメージを用いたシミュレーションにより，終始一貫した製品・生産・サービスが可能となることから，新しい技術の開発も進んでいる。

また垂直方向の通信が改善されることで，「モノのインターネット」の技術を製造において有意義かつ安全に活用する新たな可能性も生まれてくる。

プラットフォーム・インダストリー4.0参加企業，学術諮問委員会（Wissenschaflicher Beirat），運営団体であるBITKOM・VDMA・ZVEIは，技術系作業部会において共同で，単数ないし複数のリファレンスアーキテクチャモデルに必要かつ適切な標準についての評価を行い，整備する必要がある環境条件を明らかにし，研究する価値がある分野を特定した。プラットフォーム・インダストリー4.0がまとめた知見はいわばガイダンスとして，個々の企業が自らの決断により業界団体による本プラットフォームの枠外で新たな価値連鎖やビジネスモデルを提供し，それが市場で互いに競合するようになる出発点となる可能性がある。

プラットフォーム・インダストリー4.0は，同様のテーマに取り組んでおり，本プラットフォームの活動内容に関連する各種の決定機関や団体とも定期的に意見の交換を行っている。意見の交換は，指名され適宜委託された会員を通じて行われる。

学術諮問委員会の命題

3 学術諮問委員会の命題

学術諮問委員会は，学術的項目および研究方針を巡るあらゆる項目について，プロジェクトに付随する研究事業とも緊密な連絡をとりつつ，プラットフォーム・インダストリー4.0に助言を行う。諮問委員として活動しているのは，製造・自動化・情報科学・法学・労働社会学などを専門とする16名の大学教授である。

2014年のハノーバーメッセ開催にあたり（2014年4月3日時点）学術諮問委員会は命題集を発表した。この命題集はプラットフォームのウェブサイトで閲覧することができる。その命題を以下に引用するが，人間・技術・組織という三項目で構成されている。

人間

1. 人間重視の作業組織を形成するさまざまな可能性が生まれ，自己組織性や自律性にもつながるであろう。とりわけ高齢化や年齢に適った労働形態を実現するチャンスが生じる。
2. インダストリー4.0は社会技術システムとして，従業員の業務範囲を拡大し，その技能を高めて自由裁量の余地を広げ，知識習得の機会を大幅に増大させる可能性をもたらす。
3. 学習支援型の作業手段（Learnstruments）や伝達可能な労働形態（Community of Practice）によって指導および学習の生産性が向上し，IT関連技能の占める比率が増す新たな職業訓練課程が成立する。
4. 学習ツール（実際の使用に耐える学習を支援する人工物）を使うことにより，その機能が自ずと理解できる。

技術

5. インダストリー4.0システムは，ユーザーにとって分かりやすく，直感的に操作することができ，学習を助け，期待通りの反応が返ってくる。
6. ソリューションの各種パターンを誰でも利用することができ，インダストリー4.0システムを設計・実装・運用できる人の範囲が広い（インダストリー4.0バイデザイン）。
7. 製品およびビジネスプロセスのネットワーキングや個別化によって複雑さが増すが，モデリングやシミュレーション，自己組織性などにより対応する。より大きな実行可能領域をより迅速に分析できるようになり，ソリューションを見つけるのも速くなる。
8. 資源能率および資源効率を連続的に計画・監視し，自律的に最適化できる。
9. 知的製品は能動的な情報担体であり，ライフサイクルのあらゆる段階においてアドレス可能かつ識別可能である。
10. システムコンポーネントは生産手段の内部においてもアドレス可能かつ識別可能である。生産システムおよび生産プロセスのバーチャルプラニングをサポートする。
11. 新しく導入するシステムコンポーネントは，少なくとも従来のコンポーネントと同じ能力を備え，その機能を果たす互換性がある。
12. システムコンポーネントはその機能をサービスとして提供し，他者も利用できる。
13. 新たな安全文化の醸成により，信頼性が高くリジリエントで社会的に受容されたインダストリー4.0システムにつながる。

組織

14. 付加価値を有する新たな価値ネットワークおよび確立された価値ネットワークが製品・生産・サービスを統合し，作業分担の動的な変更を可能にする。

15. 協力と競合（Competition）によって経営構造および法的構造が刷新される。

16. システム構造およびビジネスプロセスは，それぞれ現行法規の枠内で可視化される。新しい法的な糸口が生じれば新たな契約モデルが可能となる。

17. 地域的な価値創造振興のチャンスが生まれる。まだ発達途上にある市場においても同様である。

本プラットフォームが同じく2014年のハノーバーメッセに合わせて発表した「研究開発項目ホワイトペーパー」では，上記命題の実現に必要となるさまざまな分野のテーマについて，その内容と目的を紹介している。また，各分野のテーマを取り上げる時期についての大まかな行程表も示されている。これらの各種テーマ分野と行程表（第4章および第5章参照）は，本プラットフォーム作業部会の活動に取り入れられている。

インダストリー4.0
実現戦略

4　インダストリー4.0実現戦略

ドイツを産業国として強化するために，プラットフォーム・インダストリー4.0では，インダストリー4.0の実現戦略策定を目指している。そのためには，業界横断的なアプローチによって技術・標準・ビジネスモデル・組織モデルなどのコンセプト作成に取り組むと同時に，大学や研究機関と中小企業・大企業の間で連携を組むことで，現場での実践をも推進してゆく。

インダストリー4.0によって新たな価値連鎖や価値ネットワークが成立し，デジタル化の進行に伴ってその自動化が行われる。その核心をなす重要項目（図参照）として

- 研究と革新
- リファレンスアーキテクチャ・標準化・規格化
- ネットワーキングされたシステムの安全性

などの項目にプラットフォーム・インダストリー4.0の該当作業部会がそれぞれ取り組んでいる。これに加えて次の項目も重要である。

- 法的環境条件の整備

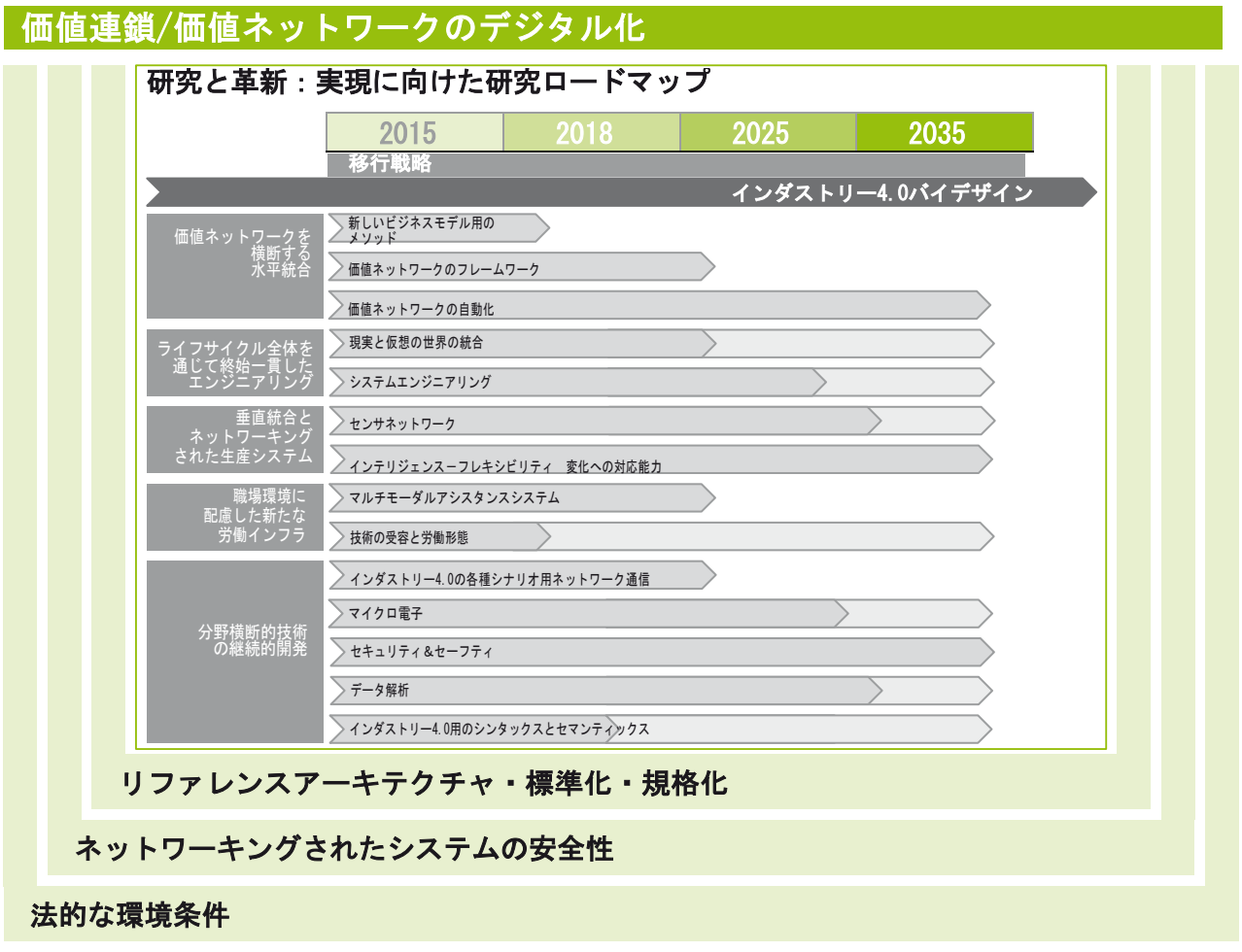


図1：インダストリー4.0の核心をなす重要項目

このテーマについてはプラットフォーム・インダストリー4.0ではなく，主にドイツ産業連盟BDIの作業部会が担当する。

研究と革新の分野においては，学術諮問委員会とも協議の上で，インダストリー4.0実現のために必要となる研究と革新のロードマップを作成し，必要な革新および研究の活動内容や，その助成について産業界の観点から協議調整する。その中で最重要事項とされているのは以下の項目である（第5章参照）：

- 価値ネットワークを横断する水平統合

  企業横断的な協働体制（納入業者，中小企業，製造業等などがその一例）の具体化に重点を置く。この項目には新たなビジネスモデルという側面やそのメソッドなども含まれる。

- ライフサイクル全体を通じて終始一貫したエンジニアリング

  この中心となるのはPLM支援型のエンジニアリングであり，製品設計と生産設計をひとつに結びつけ，価値創造全体にわたる終始一貫した支援を可能にするものである。ここで対象となる専門事項には，システムエンジニアリングとモデリング，シミュレーションの統合解析などがある。

- 垂直統合とネットワーキングされた生産システム

  この核心をなすのは生産のネットワーキングであり，さまざまな意味でリアルタイム要件を規定するものとなる。変化にも対応可能な能力と製造技術の安全性（冗長性やフォールトトレランスなど）といった必須条件の遵守・確保が可能である点が重要となる。そのためには，関連コンポーネントおよびシステム，たとえばセンサネットワークなどのさらなる改良と同時に，プレディクティブアナリティクスといったメソッドの開発も必要である。

- 職場環境に配慮した新たな労働インフラ

  成功をもたらす決定的要因が人間であることには今後も変わりがない。したがって労働の世界に生じる変化が，関係者すべて（労働組合および使用者団体等）の支持と支援を受けた前向きな進展となるよう計らうことが極めて重要である。職業訓練と社員教育の変化および改善とならんで，新たなヒューマンツーマシンシステムやアシスタンスシステム全般の導入といった側面もある。

- 分野横断的技術の継続的開発

  インダストリー4.0実現ためには，さまざまな技術的条件の整備ないし産業アプリケーション化が必要である。重要なテクノロジーは，ネットワーク通信・ブロードバンドネットワーク，クラウドコンピューティング，データアナリティクス，サイバーセキュリティ，安全な端末機器，マシンツーマシンソリューション（セマンティックス含む）などである。

リファレンスアーキテクチャ・標準化・規格化の項目においては，規格・標準を用いて，ソリューションに制約を与えることのないリファレンスアーキテクチャを作成し，それを確立することを目指している（第6章参照）。

ネットワーキングされたシステムの安全性に関する項目では，典型的な価値連鎖の例に即して，水平方向（顧客・納入業者）および垂直方向（企業内）のネットワーク内における確実なITセキュリティを保証するための理論的な考察を行っている。これは一般的な要求条件およびセキュリティ原則を特定するのに役立つ（第7章参照）。その上で反復プロセスによって具体化を行い，研究および標準化という側面も盛り込むことで，インダストリー4.0のリファレンスアーキテクチャ作成に貢献する。

法的な環境条件の項目では，新たな生産プロセスや水平方向のビジネスネットワークを法に準拠した形で構成することがその主題となる。契約法（自動化された価値連鎖における動的な契約締結）や企業データの保護，デジタル財の取り扱い，賠償責任の問題，個人関連情報の取り扱いなどがその課題となる。

研究と革新

5　研究と革新

5.1 序論

プラットフォーム・インダストリー4.0は，インダストリー4.0を巡る諸処の研究活動を，これまでより明確に統括し，内容を整理し優先順位をつけた研究アジェンダの形でまとめてゆくことを提言する。その叩き台として，本プラットフォームがこの章に示す研究ロードマップを使用する。また，このトピックが秘めるポテンシャルに相応かつ国際的な比較において十分な競争力を有する規模の連邦による助成予算を，懸案となっている研究事業実施のために用意する必要がある。助成費は，参加企業がすでにこれまで投入してきたかなりの額の資金を補完するものであり，インダストリー4.0を迅速に実現するために懸案となっている課題を的確に解決するために重要な前提条件となる。

これに加え政治が適切な措置や助成手段（最先端クラスタ，デモ用ラボ，デモ装置，デモ工場など）を通じて企業と学術界の間および規模や業種の異なる企業間のネットワーキングと協力を支援・強化・要求してゆかなければならない。

しかし詰まるところインダストリー4.0を所定のロードマップに基づき国が誘導して実現することはできない。各企業の利益や考え方が異なるため，インダストリー4.0の厳密な構想を規定することが難しいことを考えればなおさらのことである。インダストリー4.0はむしろ具体的なアプリケーション事例（便益ポテンシャルおよび価値創造ポテンシャルの分析を含む）を実現するための漸進的な変化の結果得られるものとなろう。このようにどちらかと言えば実践指向のプロジェクトに対しても，連邦政府による助成の可能性を検討することが望ましい。すなわち助成金は，新たなメソッドおよびテクノロジーの研究から大学系のデモ施設や企業系のパイロット工場への該当技術導入までの革新の全行程を支援対象とすべきである。

本章では，インダストリー4.0を巡る研究および革新にはどのような項目があるかを解説するが，その内容は学術諮問委員会の命題集にも基づくものである。これまでの成果については2014年のハノーバーメッセにおける「研究開発項目ホワイトペーパー」の中でも公表されている。それ以降も，重要事項の特定作業が続いている。以下，2015年2月の時点における更新状況をまとめた（各項目については詳細な要項が存在し，本書に記載の内容を超えたものとなっており，プラットフォーム・インダストリー4.0の各作業部会においてその更新作業が行われている）。2015年前半にはこれと併行して「研究開発項目ホワイトペーパー」の改訂版公表が予定されており，その中には該当各項目についてのさらに細かい解説が盛り込まれる。

以下，各項目について簡単に（1）研究と革新の内容，（2）期待される成果，（3）重要なステップを説明する。

5.2 研究項目：価値ネットワークを横断する水平統合

ここでいう水平統合とは，各種の価値創造プロセス（製造・物流・販売・エンジニアリング・サービスなど）の支援ないし実行のためにさまざまなITシステムを統合することを指し，製造業の企業内における統合のほか，企業の境界を越えた統合を含み，終始一貫したソリューションを実現するものである。

5.2.1 新しいビジネスモデル用のメソッド

5.2.1.1 研究と革新の内容

ビジネスモデルとは，一企業内でビジネスと価値創造がどのように機能するかを簡略化して示したものであり，すなわちどのような相手と，どのような市場で，どのような顧客層を対象に収益を上げるのかを抽象的に記述したものである。インダストリー4.0の文脈においては，新たな価値創造プロセスが生まれ，価値ネットワーク内の役割分担が変化することにより，企業内に新しいビジネスモデルが成立することになろう。

検討の対象となるのは以下の項目である：

- Go-To-Market戦略（GTM）
- 需要分析および需要創出の方法ならびにポテンシャル調査方法
- 支払および決済のモデル
- ネットワーク内の個々の関係者それぞれにとっての便益およびリスクの評価
- 法律上の事項
- 訴求と受容のシステム

5.2.1.2 研究と革新に期待される成果

ビジネスモデルに関する共通の認識が，企業横断型ネットワーキングのポテンシャルを持続的に活用してゆくための前提条件となる。さまざまな手法を統一して定着させ，ベストプラクティスや事例を（他業種におけるものも含め）体系的に掌握することが望ましい。その上で生産への適用を行い，その結果生じる影響を分析する。その際には価値ネットワーク内におけるさまざまな役割を考慮する。

以下のような成果が期待される：

- ひとつのネットワーク内において役割の異なるサプライヤそれぞれについて模範的となるGo-To-Market戦略をベストプラクティスから導出
- インダストリー4.0のニーズに合った，価値ネットワークのさまざまな側面を考慮したビジネスモデルの方向性
- 模範的な支払・決済・ライセンスのモデル
- インダストリー4.0固有の便益およびそれに伴うリスクの評価方法に関する指針
- 法律上の事項に関する指針（特にSoftware as a Service（SaaS）およびPlatform as a Service（PaaS）のService Level Agreements（SLA）における賠償責任の問題など）

5.2.1.3 重要なステップ

手法
1.4 インダストリー4.0固有の便益およびリスクの評価方法に関する指針 1.5 法律上の事項に関する指針
ソリューション
1.1 ベストプラクティスと事例掌握ならびに生産への適用 1.2 模範的Go-To-Market戦略 1.3 模範的な支払・決済・ライセンスのモデル 1.6 インダストリー4.0のニーズに合った，「価値ネットワーク」の側面を考慮したビジネスモデルの方向性 1.7 （新しい）事業戦略・ビジネスモデル・事業プロセスのパイロットプロジェクト実施
必要条件
2.3 各種組織形態向けの価値ネットワークリファレンスアーキテクチャ

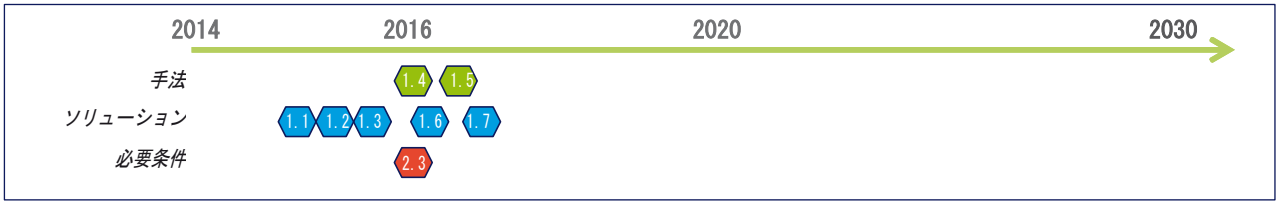


図2：新しいビジネスモデル用のメソッド研究におけるステップ

5.2.2 価値ネットワークのフレームワーク

5.2.2.1 研究と革新の内容

価値ネットワークとは，ひとつのシステムを構成する個々の価値創造プロセスと，そのプロセス同士の相互依存関係を指す言葉である。個々の価値創造プロセスは，独自に運営され，法的に独立した者によりそれぞれ実行される。プロセス実行者たちは，価値ネットワークを通じて，複雑な相互依存関係により結びついており，持続可能な経済的付加価値創造を目指す価値創造パートナーとしてひとつの利益共同体を構成する。

検討の対象となるのは以下の項目である：

- 新たな価値ネットワーク成立のための必要条件，促進要因，その影響
- 価値ネットワークのまとめ役としてのCPSプラットフォームの経済的意味合い
- 考えられる社会的脅威およびその結果生じる影響
- 価値ネットワークの組織形態，そのさまざまな要素と役割，法律上の具体化方法

5.2.2.2 研究と革新に期待される成果

価値ネットワークの具体化コンセプトを作成し，パイロットプロジェクトを実施することで，顧客・納入業者・提携先・市場などとの結びつきを強化した（新しい）事業戦略・ビジネスモデル・事業プロセスといった項目を，実践に即して検討することができる。そのために具体的なビジネスプランを作成し，いわゆる「オーケストレーション」に関する実績を積むことで，その経験を価値ネットワーク支援型CPSプラットフォームに今後求められる要件として公表する。

以下のような成果が期待される：

- 生産における価値ネットワークのフレキシブルな統合
- ネットワーク上のパートナーとその顧客の観点から見た経済的および技術的なポテンシャルの分析および評価方法
- 主に中堅企業のネットワークを通じた連携推進

- 新たな事業チャンスの開拓
- 価値創造のWin-Winパートナーシップおよびそれを通じた持続可能な「統合型」ビジネスモデル

5.2.2.3 重要なステップ

手法
2.1 統一モデルにおける個々のプロセスステップの形式仕様記述と標準（セマンティックス） 2.2 統一モデルにおけるインターフェイスおよびネットワーク全体の形式仕様記述と標準（セマンティックス） 2.3 各種組織形態向けの価値ネットワークリファレンスアーキテクチャ 2.4 連結された価値ネットワークの経済的および技術的なポテンシャルの分析および評価 2.5 実施の必要条件，促進要因，影響，進め方に関する指針 2.6 価値ネットワーク支援型CPSプラットフォームに対する要件
ソリューション
2.7 普遍的統一モデル 2.8 相関関係やモデル，必要条件，促進要因，影響などに関する基本認識
必要条件
1.6 インダストリー4.0のニーズに合った，「価値ネットワーク」の側面を考慮したビジネスモデルの方向性

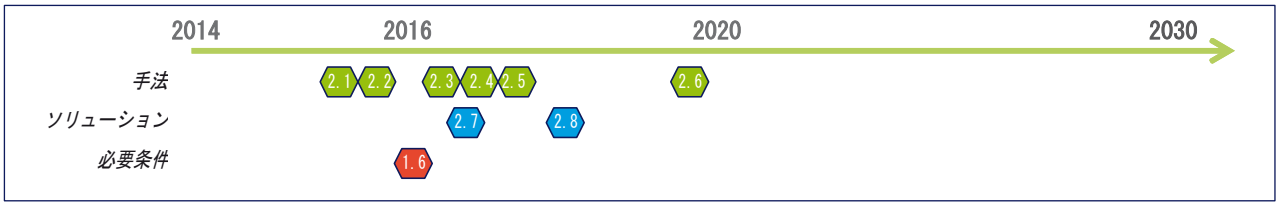


図3：研究項目「価値ネットワークのフレームワーク」の研究におけるステップ

5.2.3 価値ネットワークの自動化

5.2.3.1 研究と革新の内容

価値創造の各段階が自動化されれば，水平統合の自動化率が向上する。ここで注目に値するのは，価値創造が自動化されている段階ないし純粋に「デジタル」の世界で価値創造が行われる段階である。

検討の対象となるのは以下の項目である：

- 終始一貫した情報フロー
- モデリング・演算・シミュレーション・最適化のための各種の方式の採用
- PLM・APS・MES・SCM・ERP等のアプリケーションの統合
- グローバルな価値の流れにおける創造的従事者としての人間の関与
- マンマシンインターフェイスの構成
- 技能習得対策と移行プロセスの依存関係

5.2.3.2 研究と革新に期待される成果

価値創造の効率と柔軟性を向上させ，確実な予測を可能とすることを目指す。創造性を必要としない作業の負担から人間は解放される。生産性向上，資源効率，自動化がその焦点となる。複雑な計画プロセスの個々のステップの自動化をさらに進めることにより，その上位にある価値連鎖および価値ネットワークと事業運営を，グローバルに定義可能な目標値について最適化する。

その際には相互依存関係を考慮して，シナジー効果を上げる。そのためには，従来階層・シーケンシャル構造であった各種プロセスを統合しその一部を同期させるか，自律的に実施する必要がある。

以下のような成果が期待される：

- あらゆる事業プロセス（PLM・ERP・APS・MESなど）の直接的および間接的な相関関係と依存関係を記述するための手法
- あらゆる作業およびプロセスについて，それがグローバルに定義された目標に及ぼす影響をリファレンス化する共通の目標階層体系
- 上記相関関係および依存関係を考慮の上で，グローバル目標達成度を最適化して構成および組織化されたプロセスおよび作業
- 適用および統合が容易な自律的に記述された各種のモジュール
- 単純で直感的な表示と連続的なシミュレーションを行う機能によりユーザーを支援するツールやプログラム

5.2.3.3 重要なステップ

手法
3.1 最適化方法 3.2 戦略上の要件－目標階層体系－プロセスモデリング 3.3 複雑性の確実なコントロールと適用可能性の確保 3.4 あらゆるプロセスステップの現在の状態と予定されている状態に関する終始一貫した透過性
ソリューション
3.5 顧客・納入業者・提携先・市場などを巻き込んだ事業戦略・ビジネスモデル・事業プロセスのパイロットプロジェクト実施 3.6 価値ネットワークの終始一貫した統合とフレキシブルな連結および意思決定の最適化
必要条件
2.1 統一モデルにおける個々のプロセスステップの形式仕様記述と標準（セマンティックス） 2.2 統一モデルにおけるインターフェイスおよび情報フローの形式仕様記述と標準（セマンティックス） 2.3 各種組織形態向けの価値ネットワークリファレンスアーキテクチャ 2.8 相関関係やモデル，必要条件，促進要因，影響などに関する基本認識

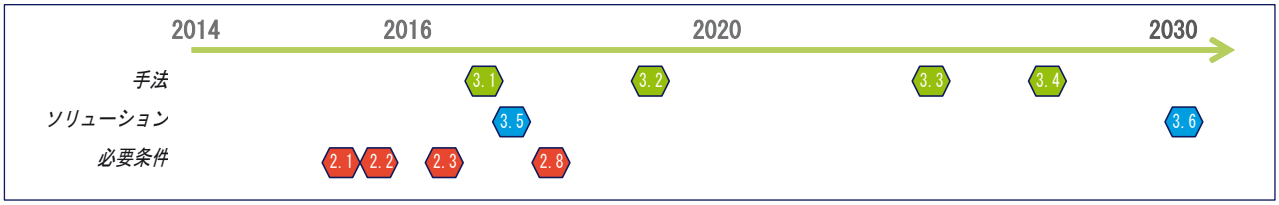


図4：価値ネットワークの自動化に関する研究におけるステップ

5.3 研究項目：ライフサイクル全体を通じて終始一貫したエンジニアリング

ある製品のライフサイクルとは，製品の開発およびそれに付随する生産システムのエンジニアリング，その生産システムを使った該当製品の生産，生産された製品のユーザーによる使用，使用後の製品のリサイクリングないし解体などを指す。このようなライフサイクルの途上で発生する情報を一貫してもれなくリンクすることが目的である。

5.3.1 現実と仮想の世界の統合

5.3.1.1 研究と革新の内容

現実の世界と仮想ないしデジタルの世界の連携というものが，インダストリー4.0においてはさらに注目を浴びるようになる。どのようなオブジェクトにもデジタルイメージ（モデル）がある。このような文脈においては，現実の世界は解決しようとする問題の所在と意思決定プロセスによって特徴づけられるのが通常である。仮想ないしデジタルの世界の主な構成要素は，シミュレーション・計画モデル・記述モデルなどである。さらに，Co-モデリングはふたつの世界のインターフェイスをさまざまなスケールで取り扱う重要なものである。

計画モデルは，複雑なシステムを構築するには必ず必要な土台となる。説明モデルによって複雑なシステムの分析が可能になり，その結果人間によるトランスファープロセスを経てソリューションや意思決定につながる。したがってどちらのモデリング手法においても仮想世界が実世界の設計に大きな影響を与えることになる。その一方でモデルの元となる状況や，要求条件ないし目標設定は実世界のものであるため，実世界も仮想世界に影響を及ぼす。

ここで必要とされるのは，学術的基盤としての機械装置製造生産技術モデリング理論である。確立されている理論や記述手段，メソッドなどは，それと結びついた情報科学の基礎技術とも合わせて，より幅の広いエンジニアリング分野での使用を踏まえて，適宜適応・拡張・併合などを行って強化する必要がある。

それぞれの対象者に合わせて，馴染みのあるその分野独特の作業法やソフトウェアツールに統合することがその鍵となる。

検討の対象となる重要事項は以下の項目である：

- 「良いモデルとは何か」（不確実性評価を含む）や「適切なモデルをどうやって見つければ良いか」，「デジタルと現実の世界でそれぞれ何を実現するのか」，また「仮想と現実の世界のインターフェイスをどう構成すればよいか」といった設問に対して堅実な解答を出すための基盤となるようなモデリング理論でなくてはならない。ただし既存のモデルも考慮する必要がある。
- モデリング理論においては，抽象化・終始一貫性・ビュー・依存関係・タイプvsインスタンス，モジュール化，モデリング深度，モデル駆動型アーキテクチャといったコンセプトや基礎概念を，セマンティックスを定義した上で規定する必要がある。
- モデリングの経済効率：モデル作成の費用に加え，ライフサイクル全体を通じたモデル利用がもたらす便益についても分析する必要がある。ここで大きな関心の対象となっているのが，モデルがそのライフタイム中にどこまで「共に成長」できるかという点である。また，既存のデータソースからのデータ蓄積も，後に一貫した割り当てを行うためのリファレンスを維持した上であれば検討の対象となる。

具体的には以下の成果を上げる必要がある：

- モデリング理論およびその理論から導出したツールおよびデータフローないし情報フローの要件（自動化ピラミッドのあらゆるレベルにおけるもの）
- 経済効率実証方法および事例
- 実用に耐えるモデリング規則
- 一般的なツール支援型のメタモデル

5.3.1.2 研究と革新に期待される成果

そのために必要な基盤となるのは，生産を取巻く機械製造・電気工学・情報科学の各分野で統一されたモデルに関する認識である。長期的な目標は，製造業の企業が経済効率よく，便益をもたらす双方向モデリングを行えるようになることである。それを通じて仮想世界の各種要素をセマンティックスの高レベルで実世界と領域横断的にリンクできるようになり，内部のタスク処理効率および意思決定の確実性が大きく向上する。

以下のような成果が期待される：

- モデリング理論およびその理論から導出したツールおよびデータフローないし情報フローの要件（自動化ピラミッドのあらゆるレベルにおけるもの）
- 経済効率実証方法および事例
- 実用に耐えるモデリング規則
- 一般的なツール支援型のメタモデル

5.3.1.3 重要なステップ

手法
4.1 複雑なシステムのモデリング理論初案，ツール要件含む 4.3 実用に耐えるアプリケーション例およびモデリング規則 4.4 個々の事例・アプリケーション例の経済効率実証方法
ソリューション
4.2 「ベスト・イン・クラス」企業の特定 4.5 モデリングフレームワークの初案 4.6 一般的なツール支援型のメタモデル
必要条件
4.a 業界横断的コミュニティの確立 4.b モデリングに対する幅広い受容 4.c モデリング深度スケーリング用のツールおよびメソッド；垂直方向および水平方向の整合性確保 4.d 作成したリファレンスアーキテクチャを利用した，実世界に対応したツール支援コンセプト

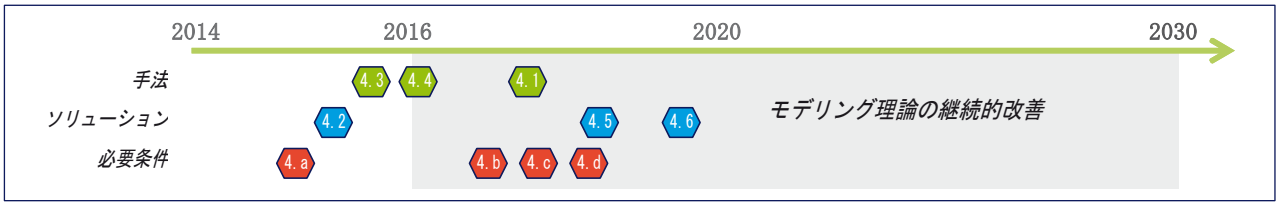


図5：ライフサイクル全体を通じて終始一貫したエンジニアリングに関する研究におけるステップ

5.3.2 システムエンジニアリング

5.3.2.1 研究と革新の内容

システムエンジニアリングは，技術システム開発のための終始一貫した分野横断的な研究項目であり，あらゆる側面を考慮する。多分野にわたるシステムがその中心となり，あらゆる開発活動を包括するものである。

検討の対象となるのは以下の項目である：

- 製品・プロセス・生産システムの統合的開発。最初からあらゆる側面を綿密に相互調整しながら開発し，製品の市場サイクルを通じて常に改良を続ける必要がある
- 設計決定の試行実験および妥当性確認を「早期」の段階において行う。意図された機能を後に機械的または電気的に実装するか，もしくはファームウェアやソフトウェア，各種のサービスを通じて実現するかという点も含む
- システム（サブシステム・機械/プロセス・生産装置・工場）および企業の境界を越えてあらゆる関連データおよびプロセスが利用可能であることと，それをスケーラブルなシステムで提供すること
- 高まってゆく複雑性とスケーラビリティを確実にコントロールするための装置およびシステムのモジュール化と再利用
- 装置およびシステムの使用経験を開発ないしエンジニアリングおよび運営にフィードバック
- 使用したメソッドによって，相互運用可能なエンジニアリングチェーンが生まれ，エンジニアリングシステムやシミュレーションシステム，運用に使用されるシステムの確実な利用（データ交換，ロールモデル，アクセス方式）およびビジネスモデル（ライセンス，決済システムなど）への組み込みがバージョンに応じて可能になる

5.3.2.2 研究と革新に期待される成果

ここで目指さなくてはならないのは，複雑なシステムの統合的で専門領域横断的な設計が，さらなる具体化の過程において，機械・電子工学・ソフトウェア工学・装置/プロセス工学などの該当分野で確立された開発手法およびそれに対応するツール環境に反映されてゆくという展開である。

システムエンジニアリングの受容度が（特に中小企業において）高まり，共同利用が増えることを目指す。そうすることで複雑性を増すインダストリー4.0システムを確実にコントロールできるようになり，エンジニアリングおよび生産の連携によって効率的かつ実効性のあるプロジェクト遂行が可能となる。

以下のような成果が期待される：

- 相互に調整されたメソッドおよび調整されたツールチェーンと開発環境
- システムおよび場所に依存しないツールの使用
- アプリケーションインターフェイスのセマンティックス
- 複雑なシステムにおける領域横断的で終始一貫した要求管理

5.3.2.3 重要なステップ

手法
5.2 実用に耐える指針および職業訓練・社員教育対策
5.3 垂直統合に沿った複雑なシステムにおける終始一貫した要求管理
5.6 業種に依存しない知的技術システム開発用リファレンスモデル
ソリューション
5.1 相互に調整された最初のメソッドセット；相互に調整された最初のツールチェーン
5.4 システム・依頼者・場所に依存しないツールの使用
5.5 アプリケーションインターフェイスのセマンティックス
必要条件
5.a 技術的要件および製造技術に関する要件を早期の開発段階で把握
4.1 複雑な自動化システムないし生産技術システムを開発するための最初のモデリング理論
5.c 技術システムの領域横断的モジュール化
5.d 生産中心的な製品記述に関する既存の標準の拡張

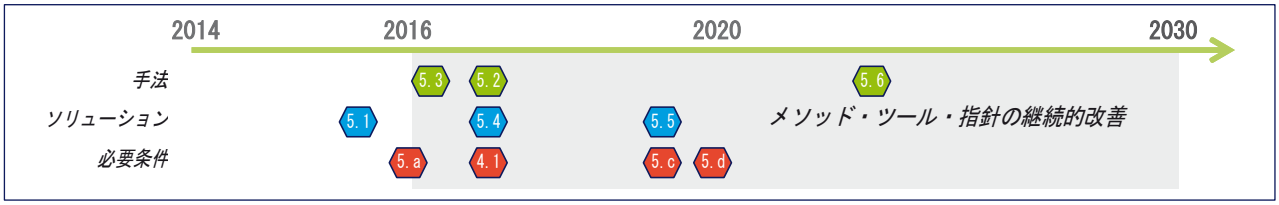


図6：研究項目「システムエンジニアリング」の研究におけるステップ

5.4 研究項目：垂直統合とネットワーキングされた生産システム

垂直統合とは，ひとつの生産システムの異なる階層レベル（アクチュエータレベルやセンサレベル，制御レベル，生産管理レベル，マニュファクチャリングおよびエクセキューションレベル，事業計画レベルなど）にあるさまざまなITシステムをひとつの終始一貫したソリューションとして統合することを指す。

5.4.1 センサネットワーク

5.4.1.1 研究と革新の内容

センサデータの分析を行おうとする最大の理由は，ひとつの（技術的）プロセスに関する情報を継続的に掌握することで，そのコントロールおよび制御または診断や警告などを行うために利用するためである。たとえば状況に応じた介入時にプロセスのパラメータを調整したり，診断時に機械の不具合を知らせたりすることが可能になる。

各種のセンサと（場合により厳しいリアルタイム条件下での）その解析結果をリンクすることが最大の課題である。

検討の対象となるのは以下の問題である：

- センサが多数の場合にデータアクイジションをどのように構成すればよいか
- データマニピュレーションを行う意義があるのはどのような場面か
- 測定された値と発生した効果の定性的および定量的な相関関係を認識し，（状態）モデルに変換するにはどうすればよいか

5.4.1.2　研究と革新に期待される成果

インダストリー4.0の各種シナリオにおいて状態依存型の監視および制御を具体化するための骨組みを作るのが目的である。センサデータ処理のメインコンポーネント（レイヤー）へのアクセスはできる限り標準化することを目指す。物理センサレベルに関する知識がなくてもセンサデータへのアクセスを可能するソフトウェアアーキテクチャが生まれることになろう。ワイヤレスセンサの組み込みにも特に留意が必要である。コミッショニングおよびコンフィグレーションは，プラグアンドプレイ方式を用いてグラフィカルかつ対話型で構成する。複数のセンサデータストリームをデータフュージョンの形で解析することを可能にする必要があり，アプリケーションごとに個別に開発する必要のないものでなくてはならない。センサネットワークの自律性をできる限り高くするために，セマンティックな記述によってセンサを拡張する（セマンティックセンサネットワーク技術）。

以下のような成果が期待される：

- システムおよび製品の状態確認用モデルが拡張・洗練され，導出される推奨対処方法の信頼性が向上する
- プロセスからフィードバックされるリアルタイムデータおよびプロセスアウトプットの質に基づく製造プロセスのオンライン制御
- 個別の事例に合わせた適応型測定戦略を品質保証に導入
- 業界横断的コミュニティの確立

5.4.1.3　重要なステップ

手法
6.1 汎用インターフェイス/メタデータによるセンサの記述を通じたセンサデータへの透過的なアクセス 6.3 自己組織性のある通信コンセプト
ソリューション
6.2 プラグアンドプレイ方式を用いた対話型コミッショニングプロセス 6.4 分散型データ解析（フォグコンピューティング）用のアルゴリズム，クラウドコンピューティング方式によるアマルガメーション
必要条件
6.a 分散型センサノードによるローカルなデータの掌握・処理・保存 6.b ネットワーキングされた生産システム（モノとサービスのインターネット） 6.c エネルギー自給型センサが利用可能であること

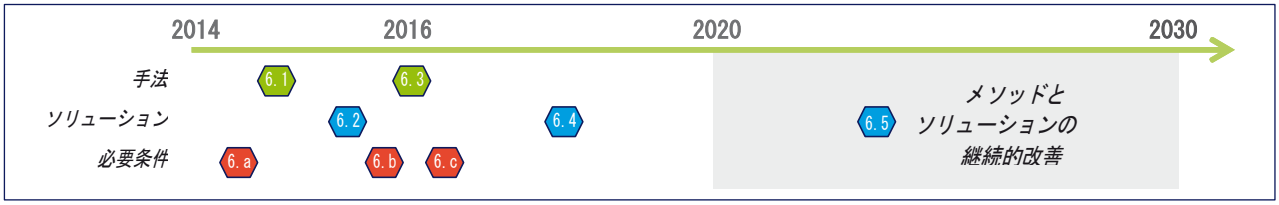


図7：センサネットワークに関する研究のステップ

5.4.2 インテリジェンス－フレキシビリティー－変化への対応能力

5.4.2.1 研究と革新の内容

知的生産システムは適応型である。すなわち，統合されたモデルの知識に基づいて周囲の環境と作用し合い，自動的に環境に適合する。堅牢でもある。開発者が想定していなかったような予期しない状況にも，常に変わりゆく環境の中にあって対応することができ，その性能水準が低下することもない。先見性も備わっている。経験知に基づき異なる要因がもたらす作用を予見して前もって対処する。そしてさらにユーザーフレンドリーでもある。ユーザーによる挙動の違いや情報のニーズが異なる点にも自動的に対応する。フレキシビリティとは，プロセスやシステムができる限り幅広い要求に応えられるように，定義された有限な枠内で構想されていることを意味する。生産環境においてこれは，人間・機械・生産システム・価値ネットワークが，異なる製品ないし各種モデルの製造にあたってフレキシブルに連携することを意味する。変化への対応能力とは，フレキシビリティの限界をシフトさせることを意味する。これによりプロセスおよびシステムの設計上の変更ないし改造が可能となる。生産環境における機械について言えば，これは新製品や新型モデル製造のための「単純な」改造にあたり，生産システムについて言うなら構造の「単純な」変更である。

検討の対象となるのは以下の項目である：

- グローバルな目標に直接および間接的に影響を及ぼすフレキシブル化および変化に対応する可能性の特定・形式化・記述
- フレキシブルで変化に対応可能な生産体制構築のための各ユニット（モジュール）のインターフェイスおよび能力の標準化
- 社会・倫理・エコロジー・人間工学への影響

生産環境における自律システムのエンジニアリングと検証；自律システムの開発者には適切な教育訓練が必要である

5.4.2.2 研究と革新に期待される成果

インテリジェンスによって製品や生産システムはこれまでなかった機能性を発揮するようになり，ユーザーの負担が軽減される。開発・エンジニアリング・保守・ライフサイクル管理などが改善され，製品および生産システムの信頼性・安全性・可用性が向上する。また，エネルギーや資材などの資源がより効率的に利用されるようになり，その結果極めてフレキシブルで容易に変化に対応できる生産プロセスおよび生産システムが可能となる。

以下のような成果が期待される：

- 生産体制内の自律性のある再利用可能なユニット（モジュール）の特定と，労働モデルに関する要件およびポテンシャルの導出
- 中央集中型および分散型のインテリジェンス用の堅牢で信頼性のあるアルゴリズム
- 生産環境における知的システム間のネゴシエーション手法
- 直感的なマンマシンインタラクション用の技術およびアプリケーション例
- フレキシブルで変化に対応可能な生産体制への移行戦略

5.4.2.3 重要なステップ

手法
7.1 フレキシブル化および変化に対応する可能性とそれが労働モデルに与える影響の分析
7.2 フレキシブルで変化に対応可能な生産体制に向けた移行戦略
7.3 自律システムのエンジニアリングおよび検証のためのメソッドと記述手段
ソリューション
7.4 直感的なマンマシンインタラクション用の技術およびアプリケーション例
7.5 生産環境における知的システム間連携の標準化
7.6 中央集中型および分散型のインテリジェンス用の堅牢で信頼性のあるアルゴリズム
必要条件
3.2 戦略上の要件－目標階層体系－プロセスモデリング
9.5 インダストリー4.0導入プロセスに該当する従業員と経営協議会を参加させるためのモデル
3.3 複雑性の確実なコントロールと適用可能性の確保

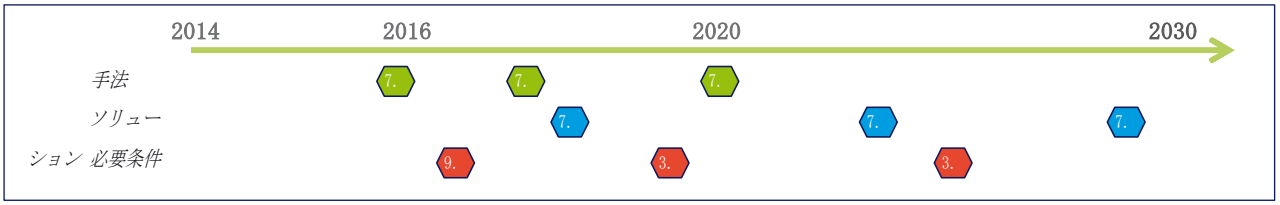


図8：インテリジェンス－フレキシビリティー変化への対応能力に関する研究のステップ

5.5 研究項目：職場環境に配慮した新たな労働インフラ

第3作業部会には，その資格および経験からいって，技術的側面からの研究開発ニーズしか特定することができない。そのため本章の内容は，学術諮問委員会から寄稿されたものである。

5.5.1 マルチモーダルアシスタンスシステム

5.5.1.1 研究と革新の内容

基本的にこの項目はマンマシンインターフェイスの人間中心的解釈を扱うものである。インダストリー4.0の一環として人間と技術のインタラクションも変化することになろう。すなわち機械が人間に合わせて変化することになる。人間が機械に合わせるということではない。マルチモーダルで操作しやすいユーザインターフェイスを備えた知的な産業用アシスタンスシステムによって，従業員の作業を支援したり，デジタル学習技術を直接職場に持ち込んだりすることが可能になる。

インタラクションの構成に関して検討の対象となるのは以下の項目である：

- 出入力のわかりやすさ
- 悪条件下でも認識可能であること
- 識別可能であること，勘違いの恐れがないこと
- 仕事への適合性
- 自己記述性
- 可制御性
- ユーザーの期待との一致

5.5.1.2 研究と革新に期待される成果

工場内における新しい協働形態を確立することを目指し，知的アシスタンスシステムによってそれを支援する。拡張現実（Augmented Reality），二重現実（Dual Reality），同期された多重の現実（すなわち工場の感覚運動・セマンティックモデルと現実の工場とのリアルタイム同期）などのメソッドおよび技術によって，複雑性の高いコンポーネントの協働的遠隔操作が可能となり，たとえばトラブルシューティングなどに役立つ。

これにより従業員の協働形態は根本から変わることになる。連携と協働は，たとえばそれに合わせたソーシャルネットワークやソーシャルメディアなどを通じ，企業や教育水準の壁を越えて可能になる。適応の容易なインタラクションシステムは多様な社員構成にも配慮したものとなり，パーソナライズされ特定の対象層向けに開発される。

以下のような成果が期待される：

- 機械による生産プロセスのシミュレーションを支援するための仮想人間モデルの統合
- 安定したシステム運用の条件となる従業員の経験知を活用かつ維持するための必要条件
- 従業員から見たシステムステータスに関する透過性の確保
- あらゆる従業員層を対象とする資格・能力取得の確保
  - デジタル学習技術の推進
  - デジタル学習技術の改善

5.5.1.3 重要なステップ

手法
8.1 作業手順のマルチモーダルな支援が有意義と思われる産業アプリケーション事例の定義 8.3 インタラクション評価用の一般的方法論
ソリューション
8.2 製品ライフサイクルのあらゆる段階におけるタスクに応じたインタラクション構成のための実用に耐える指針 8.4 マンマシンインターフェイスの構成に関する指針の明確化
必要条件
8.a 産業の適用分野におけるAugmented RealityおよびDual Realityで使用するための実用に耐える端末機器 8.b PLMシステムのネットワーキングとAR/DRアプリケーションのエンジニアリングコンセプト作成 8.c 雇用条件の弾力化を受け入れる姿勢 8.d 多様な社員構成にも配慮したインタラクションシステム構成を受け入れる姿勢 8.e あらゆる従業員層を対象とする資格・能力取得の機会の確保

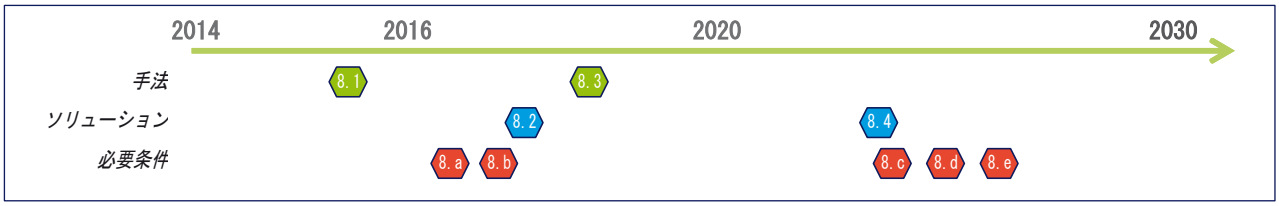


図9：マルチモーダルアシスタンスシステムに関する研究のステップ

5.5.2 技術の受容と労働形態

5.5.2.1　研究と革新の内容

インダストリー4.0は，生産に従事する社員に受け入れられる必要がある。その前提となるのは，社員にとってフレキシビリティが増し，社員の独創性や学習能力を支援するような労働条件である。「マルチモーダルアシスタンスシステム」がそのための技術的な必要条件となる。この項目の焦点には，資格能力開発や作業組織，インダストリー4.0システムの枠内での作業手段の構成なども含まれる。

検討の対象となるのは以下の項目である：

- インダストリー4.0が技術・組織・従業員の系統的な相互調整を必要とする社会技術システムであるという基本認識
- 働く人の受容・能力・成長力・幸福・健康などを促進する労働形態
- 従業員および従業員代表機関の導入プロセスへの参加

5.5.2.2　研究と革新に期待される成果

従業員の仕事の幅を広げ，その資格能力や自由裁量の余地を増強し，知識取得の機会を大きく改善することを目指す。想定されるのは，生産労働の新たな協働形態が可能となると同時に，システムに起因してその必要性が生じるという点である。したがってインダストリー4.0は，生産労働の魅力を高め，迫りつつある専門人材不足を食い止めるチャンスでもある。さらに，労働形態に関する適切な施策を通じて，従業員の高齢化という深刻さを増しつつある問題に対処するための好適な環境が整備される。

以下のような成果が期待される：

- 働く人の受容・能力・成長力・幸福・健康などを重視した作業や仕事の構造に関するコンセプト
- ひとつの職場における計画・組織・実行・検査などの作業の統合に関する提案
- 簡単な日常的作業と難しい問題解決作業の適切な比率に関するモデル
- 作業組織の支援にもなる学習促進型の作業手段
- インダストリー4.0導入プロセスに該当する従業員および経営協議会を参加させるためのモデル

5.5.2.3 重要なステップ

手法
–
ソリューション
9.1 適切な作業や仕事の構造に関するコンセプト 9.2 計画・組織・実行・検査などの作業の統合に関する提案 9.3 簡単な日常的作業と難しい作業の適切な比率に関するモデル 9.4 作業組織の支援にもなる学習促進型の作業手段 9.5 インダストリー4.0導入プロセスに該当する従業員と経営協議会を参加させるためのモデル
必要条件
–

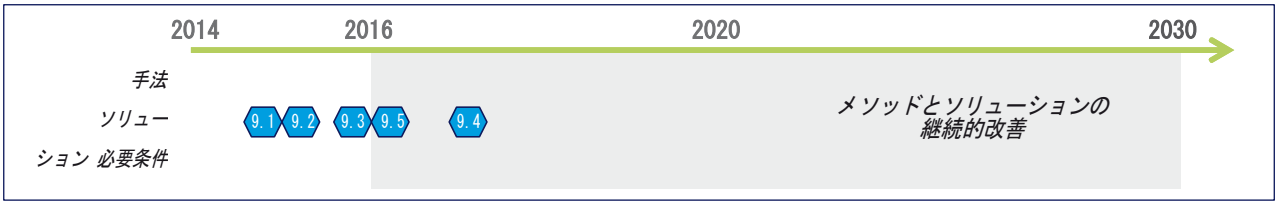


図10：技術の受容と労働形態に関する研究におけるステップ

5.6 研究項目：インダストリー4.0用の分野横断的技術

本項に記載する分野横断的技術は，決してそれがすべてというわけではなく，さらに拡張の可能性がある。さらなる技術項目を追加する際に重要なのは，該当する分野横断的技術のインダストリー4.0にとっての意味合いを明確にすることである。

5.6.1 インダストリー4.0の各種シナリオ用ネットワーク通信

5.6.1.1 研究と革新の内容

本項では，関連するサイバーフィジカルシステムの固定および移動コンポーネントのネットワーク通信を取り上げる。これは，ショップフロアおよび企業のバックオフィスシステムにおけるコンポーネントやサービスシステム，生産性システムなどで，それと連結した各サプライチェーンおよびライフサイクル各段階の枠を超えてデータ交換が可能なものを指す。

検討の対象となるのは以下の項目である：

- 事務所およびショップフロアにおける要求に応じた無線通信の利用
- 各種の異なる無線および有線通信システムとプロプライエタリシステムの共存
- 異なる無線通信システムの相互運用性
- システムコンフィグレーションが変化する場合の先を見越した作用分析
- 世界各国の利用可能な帯域での製品の使用
- 帯域幅・確定性・リアルタイム等の要求管理
- 相互運用可能なエンジニアリングチェーンにおけるスケーラブルかつ終始一貫した使用
- セキュリティとセーフティ

5.6.1.2 研究と革新に期待される成果

インダストリー4.0の生産シナリオにおける使用にあたっての要求事項を満たすため，業界横断的に使用できるネットワーキングおよび接続のソリューションを開発し評価する。

主に伝送性能，堅牢性，セキュリティとセーフティ，信頼性，経済効率，国際的展開の可能性などへの要求が本項目の対象となる。

以下のような成果が期待される：

- 相互運用性，スケーラビリティ，費用感度（高価なセンサをごく少数のみ使用する場合なども含む），要求の受容などの観点を標準に盛り込むことで，ソリューションの標準化によるインダストリー4.0の費用効率と受容の確保。標準への適合を確保する制度は，通常の製品開発プロセスに組み込むことができ，費用を増大させることのない（技術的ないし地域的な理由から認証証書の取得を義務づけることのない）制度とする。たとえばCEマークの「製造者自己宣言」のようなオープンな方式が望ましい。
- 現在および将来の可能性の評価
  - インダストリー4.0の文脈における公衆ネットワーク
  - インダストリー4.0の文脈におけるWLAN技術およびその代替として考えられる技術
  - インダストリー4.0の文脈における近距離無線技術
- 以下特定の項目に対する要求条件の特定
  - 無線ソリューション，公衆ネットワークのネットワーク技術，プロプライエタリソリューション，その代替として考えられるもの
  - アプリケーションの対象となる家屋やプロセス技術，インフラ（エネルギー・水・輸送）

5.6.1.3 重要なステップ

手法
10.1 公衆ネットワークの再設計，パブリックプライベートパートナーシップによる新たな無線技術＆周波数割当計画の導出 10.3 SDNベースのネットワークリソース仮想化 10.5 無線標準，近距離無線技術，適応型アンテナシステムの進化的改良
ソリューション
10.2 100 Gbit/s 5Gネットワークインフラが公衆ネットワークで利用可能 10.4 SDNの生産的利用 10.6 新たな無線標準，近距離無線技術，適応型アンテナシステムのI40アプリケーションへの使用
必要条件
10.a 5Gネットワークインフラおよび新たな無線標準と近距離無線技術の設計と標準化 10.b SDNベースのネットワーク仮想化用の標準ハードウェアが利用可能であること 10.c フレキシブルな無線ネットワーク用の新たなアンテナ技術の工業化 10.d 干渉の検知・抑制・回避を含む共存方式の標準化

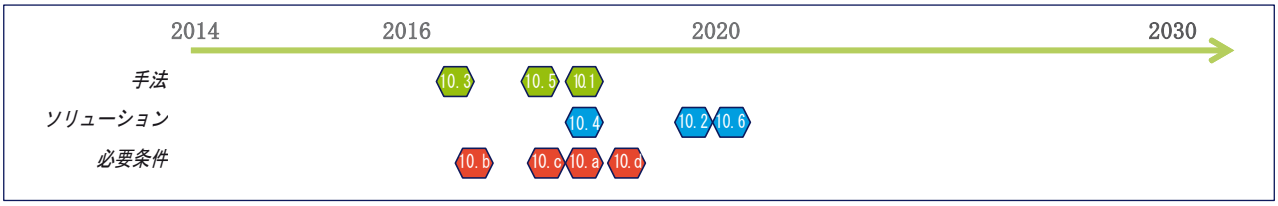


図11：インダストリー4.0の各種シナリオ用ネットワーク通信に関する研究のステップ

5.6.2 マイクロ電子工学

5.6.2.1 研究と革新の内容

マイクロ電子工学は，インダストリー4.0における生産プロセスおよび物流プロセスの知的な制御・監視・識別を行うためのCPSハードウェアの基盤である。インダストリー4.0の各種シナリオを段階的に組み上げてゆくための積み木ともいえる要素を多数有している。この意味でマイクロ電子工学は「Moore」のみならず「More than Moore」の技術をも象徴するものであり，システム統合技術（ウェーハーレベルでの3D統合，自己診断能力，エネルギー効率など）などの役割が鍵となることを考えれば，これは特に重要なものである。

最重要研究項目は：

- センサおよびアクチュエータを含むマイクロエレクトロメカニカルシステム（MEMS）
- 特殊プロセッサを含むエンベデッドシステムオンチップ，特殊なリアルタイム対応マイクロコントローラ，高性能かつ消費電力を最小限に抑えたハイテクメモリ，マルチコアアーキテクチャ
- 効率的に動作するアクチュエータシステム用のパワーエレクトロニクス
- 無線通信（ローパワー，ローレイテンシ）
- 最大限の収率を実現するエネルギーハーベスティング
- システム統合
- エンベデッドITセキュリティアーキテクチャ
- 堅牢性と耐老化性

5.6.2.2 研究と革新に期待される成果

マイクロ電子工学は，インダストリー4.0が目指すフレキシビリティや生産性向上，費用低減などの目標を達成するための鍵となる技術のひとつである。そのためには特殊な電子ハードウェアと知的ソフトウェアの連携を最適化することが前提となる。インダストリー4.0の各種シナリオの実現は，それに適したマイクロ電子コンポーネントやシステムが存在するかどうかにかかっている。したがってマイクロ電子工学のコンポーネントを新たに開発したり，既存のコンポーネントをインダストリー4.0環境における具体的な要求に適応させたりするための継続的な研究開発が必要である。

5.6.2.3 重要なステップ

手法
11.1 システム統合 11.2 堅牢性と耐老化性 11.3 最大限の収率を実現するエネルギーハーベスティング 11.4 エンベデッドシステムオンチップ，特殊なリアルタイム対応マイクロコントローラ，ハイテクメモリ
ソリューション
11.5 センサおよびアクチュエータを含むマイクロエレクトロメカニカルシステム（MEMS） 11.6 エンベデッドITセキュリティ 11.7 効率的に動作するアクチュエータシステム用のパワーエレクトロニクス 11.8 無線通信（ローパワー，ローレイテンシ）
必要条件
5.1 相互に調整された最初のメソッドセット；相互に調整された最初のツールチェーン 10.5 無線標準，近距離無線技術，適応型アンテナシステムの進化的改良

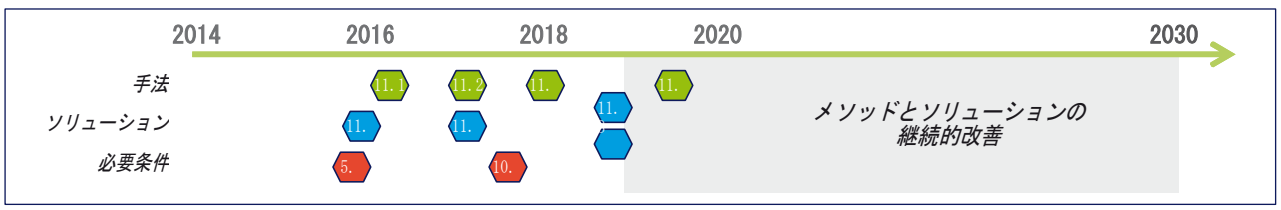


図12：マイクロ電子工学に関する研究のステップ

5.6.3 セーフティ＆セキュリティ

5.6.3.1 研究と革新の内容

セキュリティ（「情報の安全性」，英語では「information security」）とは，インダストリー4.0の装置およびシステムにおいて情報の可用性・整合性・機密性を確保するものである。セキュリティにおいて重要なのは，装置ないしその機能に影響を及ぼす危険を回避することである。特に明示的な攻撃および意図しない攻撃などもその中に含まれている。確保すべきは，運転機能をはじめ監視機能や安全機能（セーフティなど）などあらゆる機能に関する情報の安全性である。

システムのセーフティ（「機能的安全性」，英語では「functional safety」）というのは，機械や装置の機能により人間や環境に対する危険が生じないように適切な対策を講ずることを意味する。セーフティは安全操業のための安全機能の一部である。

製品・コンポーネント・インダストリー4.0装置については以下の保護項目を考慮する必要がある：

- 可用性および整合性
- 安全操業
- ノウハウの保護
- 個人情報保護

確実な身分の証明がインダストリー4.0では特に重要である。

検討の対象となる重要事項は以下の項目である：

- 安全対策の費用便益分析を含む脅威のポテンシャルとリスクの評価方法
- 対外関係および内部関係におけるインターフェイスの保護
- 装置内の通信システムの保護
- セキュリティギャップが安全操業に及ぼす危険性
- 個人情報保護等の法規定との相互作用
- セキュリティバイデザイン
- 安全ソリューションの長期有用性
- 攻撃の検知と分析

また以下のような環境条件も検討の必要がある：

- 該当する水平方向および垂直方向の価値ネットワークに合わせた安全の考え方
- 具体的なユースケースへの対応と，迅速に応用可能な結果を出すことで実用性を実証
- 「ヒューマンファクター」の考慮：透過性，ユーザビリティ，ユーザー受容性，個人情報保護

5.6.3.2 研究と革新に期待される成果

すでに現在も多様な標準や技術が存在しているが，工業環境において実践されているのはごく少数に過ぎない。その理由はさまざまだが，概していえるのは，自動化ソリューションの主たる目的はセキュリティ機能ではないということである。プロバイダにとってはセキュリティ関連プロセスによって開発および製造のコストが嵩むことになり，現状では保有していないことが多い知識を要求される。運用者にとって，セキュリティコンセプトは必要な労力と操作スタッフの受容という点においてかなり高いハードルとなる。

当事者すべての受容度を高めるためには，ユーザーにとっては操作しやすく，ツールによって開発者の負担を軽減し，効率的なセキュリティ評価メソッドを提供するようなソリューションを実現する必要がある。

以下のような成果が期待される：

- 取り扱いが簡単でユーザーフレンドリーなセキュリティメソッド
- 各種産業用のスケーラブルなセキュリティインフラ
- 個々のコンポーネントのセキュリティ特性およびそれらをひとつのインダストリー4.0装置に組み上げるという点において簡単に使用できるメソッドおよび評価方法。

ここで検討の対象となるのは「プラグ＆オペレート」や自律的な動的コンフィグレーションである

- ひとつの装置のセーフティ機能の動的な検出および評価のメソッドで，達成したセキュリティ水準がセーフティ面の残留リスクに与える影響を考慮に入れたもの
- セキュリティ標準化の準備
- セキュリティギャップが発生した場合の適切な対策の一覧作成，たとえばCERTメソッドによるもの

5.6.3.3 重要なステップ

「セキュリティ＆セーフティ」に関する研究の長期的計画について，メソッドやソリューション，またそのために必要な条件という形でのステップの定義はまだこれからである。

5.6.4 データ解析

5.6.4.1 研究と革新の内容

データ解析を行う最大の理由は，それによって（新たな）知見を得る可能性があることである。また，「アクショナブル」なデータ解析は意思決定の助けとなると同時に，自律決定（どの情報を誰に何時提供するか）にも役立ち，企業が製品の品質と生産効率を向上させ，エラーの発生を早期に認識するのを助ける。これはまた新たなビジネスモデルの基盤ともなる。そのために用いられるのは予測分析の手法である。その中には統計や機械学習，データマイニングなど多数の基礎技術が含まれている。現在と過去の測定値に加え，ソーシャルネットワークなどからのいわゆる「非構造化」データも分析し，これまで知られていなかった相関関係（ディスクリプティブアナリティクス）の導出や将来のシステム挙動ないし効果の推測（プレディクティブアナリティクス）を行う。新しく得た知見に基づいて，最終的には異なる行動の選択肢の評価が可能となり，システム・プロセス・戦略の継続的最適化（プリスクリプティブアナリティクス）につながる。

データ解析に基づく推奨対処方法または直接の対策の導出がその本来の課題である。

「データ解析」の項目には以下の点が含まれる：

- データマニピュレーション
- ステートディテクション
- プログノスティックアセスメント
- アドバイザリージェネレーション

5.6.4.2 研究と革新に期待される成果

データ解析使用の基準を策定し，以下の原理を実現する：

- 具体的な（物理）データソースを知らない状態でのデータへのアクセス（カプセル化ないし仮想化）
- プラグ＆ユーズ方式を用いた標準インターフェイスによる新たなデータソースの接続（セマンティック記述）
- 業界横断的価値ネットワークにおけるデータの利用
- 新たなアプリケーション事例が導出できるような幅広く連続的に拡張可能なプロセス基盤を作成する
- 法的安定性（誰がどのデータおよびデータから得られるどのような知見に対してどのような権利を有するのか）

さらに，ソフトウェアアーキテクチャや然るべきインターフェイスによって，複数のデータストリームをひとつのメタレイヤーにおけるデータフュージョンの形で解析することが可能となり，アプリケーションごとに個別に開発する必要がないような原理を構築する。

- 将来の状態の予測を可能にするような状態記述モデルを構築する
- 常に増え続けるデータの量を効果的かつ効率的に解析できるような方式およびアルゴリズムを開発する

5.6.4.3 重要なステップ

手法
13.2 生産環境におけるデータ解析利用に関するアプリケーション指針 13.4 生産プロセスをオンラインで調整・最適化するためのアナリティクス技術
ソリューション
13.1 データ解析の技術とアプリケーション例 13.3 分散型データ解析（フォグコンピューティング）用のアルゴリズム，クラウドコンピューティング方式によるアマルガメーション 13.5 複雑な製造プロセスの動的制御，経営プロセスとの垂直統合
必要条件
13.a データの所有権と処分権の状況を法的に明確化 13.b ディスクリプティブアナリティクス・プレディクティブアナリティクス・プリスクリプティブアナリティクスの基礎理論

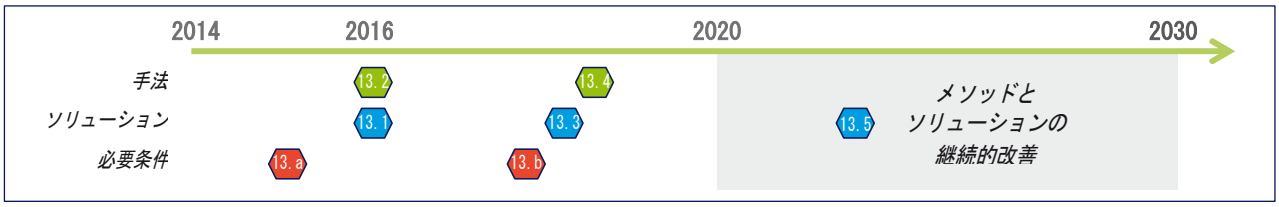


図13：研究項目「データ解析」の研究におけるステップ

5.6.5 インダストリー4.0用のシンタックスとセマンティックス

5.6.5.1 研究と革新の内容

インダストリー4.0の各種シナリオを実現するためには，参加するオブジェクト（たとえば機械，機械のコンポーネント，製品，製品記述，デジタルファクトリーでいう各種リソースなど）を，行動するサブジェクト（たとえば人間，ソフトウェアツール，ソフトウェアエージェント，制御システム，ソフトウェアサービス）が解釈できること，すなわち識別して理解できることが前提となる。そのためには，それぞれオブジェクトの該当する特性を，モデルにおけるプロパティの形で記述し，オブジェクトのタスクをロールとの関連において記述する必要がある。その基盤となるのは各種の情報モデルである。生産環境においては，コンピュータ処理を可能にするために，（データ）モデル，モデルシステム，説明モデル，計画モデル，コンポーネントモデルなどが必要となる。

シンタックスは，文書やデータの記述に使うことが許される有効な記号（文字や数字，特殊文字，図形記号など）と，その記号を適正に組み合わせて文字列を構成する方法を記述したものである。

セマンティックスは，記号とモデルを関連づけるもので，それにより文字列ないしデータが意味をもつようになり，データが情報になる。そのような関係にあたるのが，たとえばファイル内のある特定の文字列があるモデルの特定のプロパティを記述するという取り決めで，このプロパティの属性をさらに細かく記述し，その属性を持つことが許されるインスタンスを記述する。さらにプロパティと属性の相互依存関係も記述する必要がある。

5.6.5.2 研究と革新に期待される成果

目標は，インダストリー4.0の各種シナリオ用に，形式手法によるコンピュータ処理可能な形態の記述を共通のセマンティックスとして開発することで，アプリケーションと使用のレベルにおいて領域特化型の「言語」仕様を規定し，すべてのオブジェクト，サブジェクト，そのリンク（すなわちプロセス・通信・価値創造のネットワーク）を統合して利用できるようにすることにある。そこで重要となるのは，情報フローの終始一貫性を価値連鎖内および価値連鎖間で確保することと，前述した既存の規格を基盤として，それをさらに改良し，規格の欠陥が見つかった場合には補正することである。

- セマンティックスとシンタックスにより，データの保存・通信・処理の製造者横断的相互運用性のための大前提が整備されることになる。
- 規格化されたセマンティック記述は，価値連鎖の自己最適化挙動や自動化の基盤となる。
- これによりモデルを完全なライフサイクルに組み込むことが可能となる（製品・プロセス・資源の記述をセマンティックスとしてエンジニアリングで利用できるため）。
- シンタックスとセマンティックスを用いることで，ジェネリックツールないしジェネリックツール機能の作成が可能となる。
- シンタックスとセマンティックスにより，インダストリー4.0コンポーネントのプラグアンドプロデュース機能が可能になり，フレキシビリティや適応能力が得られる。

課題となるのは，インダストリー4.0用のシンタックスとセマンティックスの具体化において迅速に成果を上げつつ，できるかぎり幅広い適用範囲を（インダストリーフットプリントとして）実現することである。

5.7 研究項目の相互依存関係と相関関係

それぞれの研究項目は独立したものではなく，研究結果には相互依存関係がある。たとえばある研究項目で新しい成果があれば，ほかの項目の研究にも影響を与える。現在第3作業部会では学術諮問委員会と協力して各研究項目の相互作用と相関関係についての分析を行っているところである。分析にはガウゼマイヤー教授のシナリオ分析法を採用している。分析の結果は年内に公表の予定であるが，すでに現在の時点でも，以下の項目の研究結果がそれぞれ他の研究結果に大きな影響を与えるであろうことが判明している。

- 「フレキシビリティ，インテリジェンス，変化への対応能力」
- 「センサネットワーク」
- 「価値ネットワークのフレームワーク」
- 「セキュリティ＆セーフティ」

5.6.5.3 重要なステップ

手法
14.8 インダストリー4.0におけるシンタックスとセマンティックスの取り扱いに関するアプリケーション指針
ソリューション
14.1 シンタックスとセマンティックスを巡る標準化/規格化の現状分析 14.2 シンタックスとセマンティックスを巡る関連コンセプトの現状分析と評価 14.3 シンタックスとセマンティックスに関するインダストリー4.0の要求事項 14.4 アプリケーション事例と価値連鎖に基づく研究項目の特定 14.5 規格の欠陥認識とそれに応じた標準化の必要性を標準化/規格化ロードマップに盛り込む 14.6 相互運用性の実証モデルを選択し実現 14.7 既存の通信標準への統合コンセプト，ソフトウェアツール設計の拡張
必要条件
14.a アプリケーション事例と価値連鎖から導出したデータと情報のモデルに対する要求条件

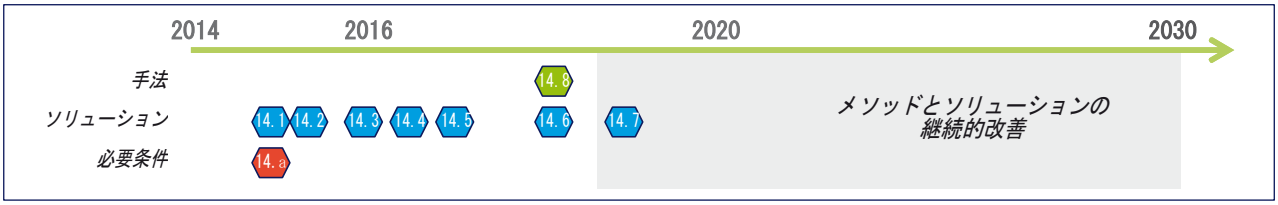


図14：インダストリー4.0用のシンタックスとセマンティックスに関する研究のステップ

リファレンスアーキテクチャ
標準化・規格化

6　リファレンスアーキテクチャ・標準化・規格化

本章では複数の機関[2]の協力によって得られた，インダストリー4.0の基本的なリファレンスアーキテクチャと，そこから導出される標準化と規格化の必要性に関する検討結果を総括する。

プラットフォーム・インダストリー4.0は，幾つもの部会による活動の調整役として，路線の統一を図る立場になった。すなわち本プラットフォームは，異なる機関や団体が協調行動をとるように計らうという本来の役割を果たした。したがって，以下に紹介する幅広い支持を得た検討結果は，ドイツ産業の競争力を維持するための重要な一歩となる。

6.1 序論

インダストリー4.0のリファレンスアーキテクチャに関する基本的な考え方のひとつは，さまざまな側面をひとつの共通モデルとしてまとめようというものである。工場内の垂直統合とは，自動化機器や各種サービスなどの生産手段を相互にネットワーキングすることをいう。インダストリー4.0では新しい側面として製品や半加工品がその中に加わることになる。そのモデルにはこの点が反映されていなくてはならない。しかしインダストリー4.0は決してそれだけでは終わらない。価値連鎖全体を通じて終始一貫したエンジニアリングというのは，生産手段や半加工品を巡って発生する技術データ・管理データ・商業データなどの整合性が価値連鎖のあらゆる部分において保たれ，ネットワークを通じていつでもアクセス可能であることを意味する。インダストリー4.0の第三の側面となるのが，各地の工場の範囲を超えた価値ネットワークの水平統合で，価値ネットワークの動的形成が可能となる点である。

以上のような点をひとつのモデルとしてまとめるというのが，解決しなければならない課題であった。さらに，ミリ秒単位で走査を行う制御系，共通の価値ネットワーク内にある複数の工場間の動的な連携を，それに伴う新たな商業的問題点も踏まえて，一つのモデルとして表現することが目的である。ここで重要なのは，さまざまなアプリケーション領域で異なる視点を理解し，その本質的な部分を捉えて，共通のモデルとして一体化することであった。

そのため，リファレンスアーキテクチャモデルRAMI4.0本来の作業に取りかかる前にまず，既存の理論や手法について鳥瞰する必要があった。すでに存在する一連の手法が有用であることはすぐに判明したが，その多くは上述したインダストリー4.0の総合的観点の一部のみを扱ったものであった。具体的には以下の手法を詳細に検討した：

コミュニケーションレイヤー実装のための手法

- OPC UA：基盤となる標準：IEC 62541

インフォメーションレイヤー実装のための手法

- IEC Common Data Dictionary（IEC 61360Series/ ISO13584-42）
- eCl@ss準拠のプロパティ，クラシフィケーション，ツール
- Electronic Device Description（EDD）
- Field Device Tool（FDT）

ファンクショナルレイヤーとインフォメーションレイヤーの実装のための手法

- 統合技術としてのField Device Integration（FDI）

2　VDIおよびVDEの測定・自動化技術協会（GMA）で働く専門家の方々に各種手法の検討にご協力いただいた。特に7:21「インダストリー4.0」および7:20「サイバーフィジカルシステム」の両専門委員会にお礼申しあげる。
これと並行してZVEIにも組織内ミラー委員会としてSG2が設立され，共同での検討に寄与している。SG2にはDKE（ドイツ電気技術委員会）の代表者も参加しており，規格化という点も共同検討の対象になった。

終始一貫エンジニアリングの手法

- AutomationML
- ProSTEP iViP
- eCl@ss（プロパティ）

その第一歩としてまず，これらの手法が次の項で紹介するリファレンスアーキテクチャモデルに合うものであるかどうかを検討した。その答は基本的に肯定的なものであるが，各種のコンセプトやメソッドについてはさらに詳細な検討が必要となる。

6.2 インダストリー4.0リファレンスアーキテクチャモデル（RAMI4.0）

インダストリー4.0を巡る議論においてはまったく異なるさまざまな利益が交錯する。プロセス自動化から工場自動化に至る各業界の標準は異なり，情報通信技術や自動化技術などの各種テクノロジー，BITKOM，VDMA，ZVEI，VDIなどの団体やIECおよびISO等の規格化団体とその国内機関であるDKEないしDINなどが関与している。

インダストリー4.0のためにどのような標準やユースケース，規格などが必要となるのかについて同じ認識を共有するために，統一されたアーキテクチャモデルをリファレンスとして作成し，それに基づいて相関関係や詳細について話し合う必要が生じた。

その結果生まれたのがインダストリー4.0リファレンスアーキテクチャモデル（RAMI4.0）である。

その中にはインダストリー4.0の主要な側面が盛り込まれている。これはIEC 62264の階層の最下段に製品ないし半加工品（「Product」）を追加し，最上段の一つの工場よりも上に「Connected World」のレベルを追加するものである。横軸は装置ないし製品のライフサイクルを表し，タイプとインスタンスを区別するという点も反映されている。そして六つのレイヤーによってインダストリー4.0コンポーネントのデジタルイメージを構造化して記述する。

したがってリファレンスアーキテクチャモデルの特徴は，ライフサイクルと価値連鎖とを組み合わせて階層構造によってインダストリー4.0コンポーネントを定義している点にある。

これによりインダストリー4.0環境を記述する際のフレキシビリティが最大限確保される。この方法ではまた機能のカプセル化を有意義な形で行うことが可能である。

よって，リファレンスアーキテクチャモデルを用いて極めてフレキシブルなコンセプトを記述し実装するための必要条件が整っている。尚このモデルでは，現在の状況からインダストリー4.0の世界への段階的な移行や，特殊な制約や要求を伴うアプリケーション領域の定義なども可能となる。

リファレンスアーキテクチャモデルはDIN SPEC 91345として規格化される予定である。

6.2.1 要求条件と目標

目標

インダストリー4.0は「モノとサービスのインターネット」を特化させたものである。およそ15種類の業種を考慮に入れる必要がある。リファレンスアーキテクチャモデルによってタスクやプロセスを分解して整理することができる。モデルによって状況がわかりやすくなり，標準化や規格化などに関する的確な議論が可能になることが意図されている。また，該当する既存の標準や規格をマッピングできるようにすることで，拡張や修正の必要があるケースや，規格および標準が欠如している部分などを可視化する。そうすれば重複している箇所などもおのずと見えるようになり議論が可能となる。同一もしくは類似の事項について複数の標準が存在することがモデルの検討から判明した場合には，リファレンスアーキテクチャモデルにおいて優先する標準について議論すればよい。

目指すは，できる限り少ない標準で済ますことである。

標準の遵守

選択した規格および標準については，その中に記述されているコンセプトやメソッドがインダストリー4.0環境におけるアプリケーション用にどの程度適したものかについての検証を行う。初期のインダストリー4.0アプリケー

ションでは，規格ないし標準の一部のみを遵守すれば十分である場合も考えられる。その場合には，インダストリー4.0のために必要不可欠な製造者横断的ソリューションの具体化および導入が加速し，またそれほど規模が大きくない企業にとっても，インダストリー4.0の実践および適合をより迅速にやり遂げる可能性が生じる。

ユースケース

リファレンスアーキテクチャモデルではまた，インダストリー4.0のユースケースをマッピングすることで，たとえば各ユースケースに必要な規格や標準を特定することもできる。

リレーションのマッピング

リファレンスアーキテクチャモデルではさまざまな項目をサブスペースとして表現することができる。このようなサブスペースなどのリレーションを電子的に把握して加工できることがインダストリー4.0最大の利点である。

上位規則の定義

リファレンスアーキテクチャモデルでは，上位レベルでのインダストリー4.0実装を実現するための規則を導出することが可能になる。

目標一覧：

- リファレンスとしてのわかりやすくシンプルなアーキテクチャモデル
- 既存の規格および標準のマッピング
- 規格および標準の欠陥の特定と補正
- 重複箇所の特定と優先ソリューションの規定
- 使用する規格および標準の数を最小限に抑える
- インダストリー4.0の部分的実現の迅速化に適した規格ないし標準の部分を特定（「I4.0-Ready」）
- ユースケースコンテンツのマッピング
- リレーションのマッピング
- 上位規則の定義

6.2.2 リファレンスアーキテクチャモデルの簡単な説明

インダストリー4.0スペースを最も良く表すことができるのは三次元モデルである。このモデルはその根本において，欧州のスマートグリッドコーディネーショングループ（SG-CG）が定義し，世界的にも認められているスマートグリッドアーキテクチャモデル（SGAM[3]）に基づくものである。インダストリー4.0の必要条件に即して修正および拡張を行っている。

縦軸には，データイメージや機能的記述，通信挙動，ハードウェア/アセット，ビジネスプロセスなどの異なる視点を表すためにレイヤー/層を用いている。これは，複雑なプロジェクトを整理しやすいユニットとしてクラスタリングするというITの考え方に沿ったものである。

もうひとつの重要な基準となるのが，製品ライフサイクルとその中に含まれる各種の価値連鎖である。この状況については横軸に表してある。これによりリファレンスアーキテクチャモデルでは相互依存関係もうまく表すことが可能で，たとえばライフサイクル全体を通じて終始一貫したデータ収集なども表すことができる。

第三の重要な基準は第三の軸として表されており，工場/装置内の機能および責任のマッピングである。これは機能的な階層であって，従来の自動化ピラミッドにおけるデバイスのクラスや階層レベルとは異なる。

3 CEN/CENELEC/ETSI SG-CG, Overview of SG-CG Methodologies, Version 3.0, Annex SGAM User Manual, 2014

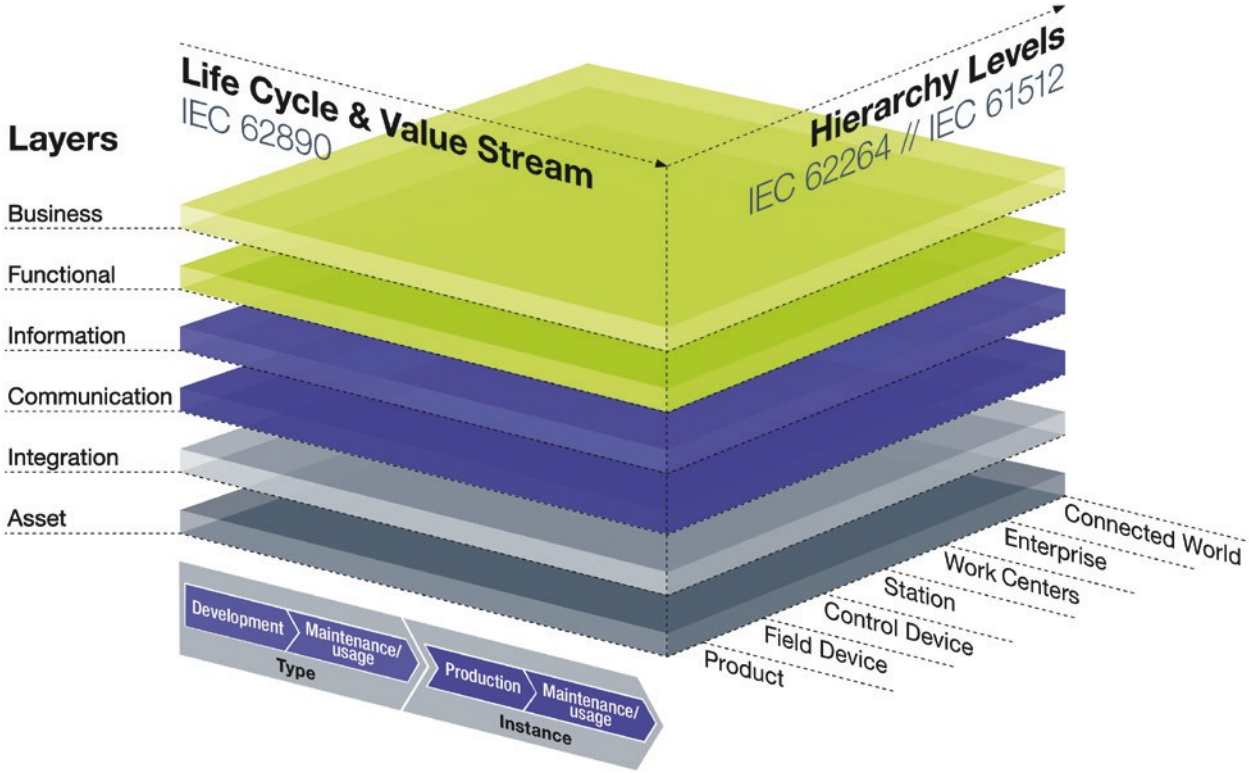


図15：リファレンスアーキテクチャモデル / Reference Architecture Model Industrie 4.0 (RAMI 4.0)

6.2.3 リファレンスアーキテクチャモデルの層（レイヤー）

スマートグリッドモデル（SGAM）が，ここで記述しようとする状況を表すのに良い手がかりとなる。このモデルは，発電から送電と配電を経て消費者に至るまでの電力系統を扱ったものである。インダストリー4.0では製品開発と生産のシナリオが中心となる。すなわち，開発プロセスや生産ライン，製造機械，フィールド機器，そして製品自体がどのような構成になっているか，どのように機能するのかを記述できなくてはならない。

それがどのようなコンポーネントであっても，機械・製品の別に関わりなく，関心の対象となるのは情報技術および通信技術に関する機能のみではない。たとえばひとつの機械全体のようなシステムのシミュレーションを行うには，そのケーブルやリニア駆動装置，また機械的な構造なども合わせて考慮する。これらの要素は能動的な通信は行えないものの，現実の一部である。その情報もバーチャルイメージとして存在する必要がある。そのためには，たとえば2Dコードなどを用いて，データバンクのエントリーと結びつける。

機械やコンポーネントと工場のいずれをも記述しやすくするために，SGAMのコンポーネントレイヤーをアセットレイヤーに置き換えてモデルの最下層として挿入し，その上にインテグレーションレイヤーを新たに追加した。このレイヤーによってバーチャルイメージにおけるアセットのデジタル実装が可能になる。コミュニケーションレイヤーは，データおよびファイルのプロトコルや転送を扱い，インフォメーションレイヤーには関連するデータが含まれ，ファンクショナルレイヤーには必要なすべての（形式手法で記述された）機能が入っており，ビジネスレイヤーには該当するビジネスプロセスがマッピングされている。

備考：*各層内では連関性が強く，各層間には弱いつながりがあるものとされている。イベントのやりとりができるのはふたつの隣接する層の間か，ひとつの層内に限られる。*

複数のシステムをより規模の大きなシステムとしてひとつにまとめる。ただし個々のシステムも，それをまとめた全体のシステムもリファレンスアーキテクチャモデルに適合したものでなくてはならない。各層の内容には互換性がなくてはならない。

次に各層および各層間のリレーションについて解説する。

6.2.3.1 事業層（ビジネスレイヤー）

- 価値連鎖における各機能の整合性確保
- ビジネスモデルおよびそれから生じる総合プロセスのマッピング
- 法律・規制等の環境条件
- システムが遵守しなければならない規則のモデリング
- ファンクショナルレイヤーの各種サービスのオーケストレーション
- 異なるビジネスプロセスを連結するエレメント
- ビジネスプロセスを先に進めるためのイベントの受け取り

ビジネスレイヤーは，たとえばERPのような具体的なシステムを表すものではない。ERP機能でプロセスの文脈において作動するものは，通常ファンクショナルレイヤーに含まれる。

6.2.3.2 機能層（ファンクショナルレイヤー）

- 各種機能の形式仕様記述
- さまざまな機能の水平統合用プラットフォーム
- ビジネスプロセスを支援する各種サービス用のランタイム環境およびモデリング環境
- アプリケーションおよび専門機能のランタイム環境

ファンクショナルレイヤー内では，規則・意思決定ロジックが生成される。この規則や意思決定ロジックは，アプリケーション事例によって，下位の層（インフォメーションレイヤーまたはインテグレーションレイヤー）で実行することもできる。

遠隔アクセスや水平統合が行われるのはファンクショナルレイヤー内部のみである。これにより，プロセスの情報と状態の整合性および技術レベルの統合が確保される。保守の目的では，アセットレイヤーおよびインテグレーションレイヤーへの一時的なアクセスも可能である。

そのような可能性を利用するのは，下位の層にのみ関連する情報やプロセスにアクセスしようとする場合が主である。センサ・アクチュエータのフラッシュメモリプログラムアップデートや診断データの読み取りなどがその例である。保守のための一時的な遠隔アクセスは，恒常的な機能統合や水平統合とは関連がない。

6.2.3.3 情報層（インフォメーションレイヤー）

- イベントの（前）処理用ランタイム環境
- イベント関連規則の実行
- 各種規則の形式仕様記述
- コンテキスト：イベント前処理

単数または複数のイベントから規則に従って単数または複数の新たなイベントが生成され，それがファンクショナルレイヤーでの処理をトリガする。

- 各種モデルを表すデータの残留
- データ整合性の確保
- さまざまなデータの整合のとれた統合
- 新しく，より価値のあるデータの取得（データ，情報，知識）
- サービスインターフェイスを通じた構造化データの提供
- イベントの受け取りと，ファンクショナルレイヤーで利用可能なデータに合わせた変換

6.2.3.4 通信層（コミュニケーションレイヤー）

- 統一したデータフォーマットを用いたインフォメーションレイヤーに向けた通信の統一
- インテグレーションレイヤー制御用のサービス提供

6.2.3.5 統合層（インテグレーションレイヤー）

- 物理/ハードウェア/文書/ソフトウェアなどのアセットのコンピュータ処理可能な情報の提供
- 技術プロセスのコンピュータ支援制御
- アセットからのイベントの生成
- RFIDリーダーやセンサ，HMIなどのITに連結されたエレメントを含む

人間とのインタラクションも，マンマシンインターフェイス（HMI）等を通じてこのレベルで行われる。

備考：現実の重要なイベントは必ず，バーチャルのイベント，すなわちインテグレーションレイヤーのイベントがあることを示している。現実に変化があると，そのイベントは適切なメカニズムによりインテグレーションレイヤーに報告される。重要なイベントはコミュニケーションレイヤーを通じてインフォメーションレイヤーに対するイベントを生じさせることがある。

6.2.3.6 物体層（アセットレイヤー）

- 現実のイメージを表す，たとえば直進軸や金属板部品，文書，回路図，アイデア，アーカイブなど
- 人間もまたアセットレイヤーの一部であり，インテグレーションレイヤーを通じて仮想世界に結びついている。
- QRコードなどを通じたアセットの統合層との受動的接続

6.2.4 ライフサイクルと価値連鎖（Life Cycle & Value Stream）

ライフサイクル

インダストリー4.0は，製品・機械・工場等のライフサイクル全体を通じ，大幅な改善を行うチャンスをもたらす。相関関係やつながりを可視化し，標準化するため，リファレンスアーキテクチャモデルの第二軸はライフサイクルおよびそれと結びついた価値連鎖を表している。

ライフサイクルの分析には，IEC 62890のドラフトが非常に参考になる。その中ではタイプとインスタンスを明確に区別することが分析の要となる。

タイプ：

タイプとは常に，アイデアの発想とともに生まれるものであり，すなわち「デベロップメント」段階における製品の誕生とともに成立する。デベロップメントとは，指示・開発・試験から試作品第一号およびプロトタイプの製造までを意味する。つまり，この段階において製品や機械などのタイプが成立する。すべての試験および妥当性の確認が終了すると，そのタイプの量産ができるようになる。

インスタンス：

一般的なタイプに基づき，生産によって製品の製造が行われる。そして製造された製品のひとつひとつが，それぞれこのタイプのインスタンスとなり，一意的な製造番号などがつけられる。各インスタンスは販売に回されて顧客に出荷される。顧客にとっては，製品は差し当たってタイプにすぎない。それがインスタンスになるのは，製品が具体的な装置に取り付けられた時点である。タイプからインスタンスへの変化が何度も繰り返される可能性がある。

販売段階から改良すべき点がフィードバックされて，製品の製造者側でタイプ関連書類の修正につながることがある。新しくなったタイプによって再び新しいインスタンスを製造できるようになる。したがって，使用と整備の対象となるという点では，タイプも個々のインスタンスと変わりがない。

例：
新しい油圧バルブの開発は新しいタイプにあたる。バルブの開発が行われ，最初の試作品を作って試験を行い，最後に第一世代のプロトタイプを生産して，妥当性を検証する。妥当性確認が完了すると，このタイプの油圧バルブの販売が許可される（販売カタログにマテリアル番号および/または製品名を記載）。これにより量産も始まる。
量産においては製造された油圧バルブそれぞれに一意的な表示（製造番号）がつけられて，かつて開発した油圧バルブの一インスタンスとなる。
販売されたフィールドの油圧バルブ（インスタンス）に関するフィードバックが，たとえば機械設計と図面の小さな変更およびバルブのファームウェアのソフトウェア修正につながる。このような変更はタイプの変更であり，すなわちタイプ関係書類に反映されて，再び製造販売の許可が行われると，変更を加えたタイプの新しいインスタンスが生産されるようになる。

価値連鎖：

価値連鎖のデジタル化と連結は，インダストリー4.0による大きな改善の可能性を孕んでいる。ただし，機能横断的に連結することが決定的な意味合いを持つ。

物流データを組み立て工程において利用することができ，工場内物流は受注状況に即した自己組織型となる。購買ではリアルタイムの在庫状況や，納入部品が特定の時点にどこにあるかを見ることができる。顧客には発注した製品の製造工程における完成度がわかる。購買・受注オーダー計画・組み立て・物流・メインテナンス・顧客・納入業者等を結びつけることで大幅な改善の可能性がある。そのためライフサイクルを，それに含まれる価値創造プロセスと合わせて考える必要があり，それもひとつの工場だけを分離して考慮するのではなく，全工場とエンジニアリングから納入業者，顧客までを含めたすべてのパートナーを合わせて考えるのである。

なお，価値連鎖については，VDI/VDE GMA専門委員会7.21が発表した「価値連鎖」[1]も参照されたい。

6.2.5 階層レベル（Hierarchy Levels）

リファレンスアーキテクチャモデルの第三軸は，ある状況のインダストリー4.0内での機能的な位置づけを記述するものである。これは実装についてのものではなく，純粋に機能的な割り当てにすぎない。

工場内の位置づけにあたりリファレンスアーキテクチャモデルがこの軸について参考にしているのはIEC 62264およびIEC 61512の規格である（図参照）。プロセス技術から工場自動化まで可能な限り数多くの業種について統一した考察ができるように，その中に記載されている選択肢の中から「エンタープライズ」，「ワークセンター」，「ステーション」，「コントロールデバイス」という概念を用いた。

インダストリー4.0には，コントロールデバイス（中央制御等）のみでなく，一台の機械や装置の内部についても考慮することが決定的に重要な意味をもつ。そのためコントロールデバイスの下位に「フィールドデバイス」を追加した。これはたとえば知的センサなどの知的フィールド機器の機能的レベルである。

さらにインダストリー4.0では製品の製造のための装置に加え，製造する製品自体も分析のために重要となる。したがってレベルの下段にはさらに「製品」を挿入してある。こうすることでリファレンスアーキテクチャモデルにおいて製造する製品と生産装置をその相互依存関係とともにむらなく分析することが可能となる。

階層レベルの最上段にもやはり追加した項目がある。というのは，上記のIEC規格はいずれもひとつの工場内の各レベルしか表示していないからである。しかしインダストリー4.0ではさらに一歩進んで，工場の連携や社外エンジニアリング事務所，納入業者，顧客等との協働なども記述する。そのため分析のためにエンタープライズレベルの上にさらに「コネクテッドワールド」のレベルを挿入した。

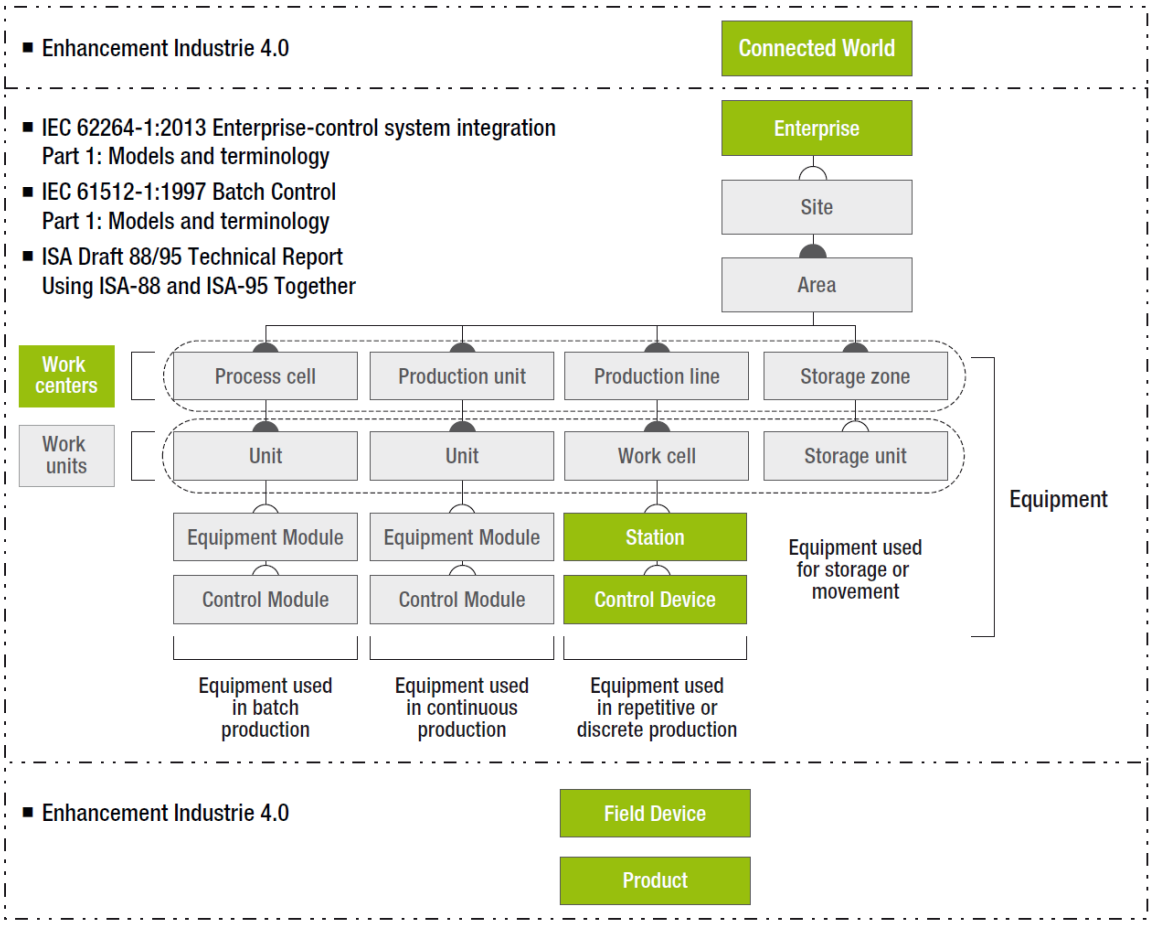


図16：リファレンスアーキテクチャモデルRAMI4.0の階層レベルの導出

6.3 インダストリー4.0コンポーネントのリファレンスモデル

以下に解説するインダストリー4.0コンポーネントリファレンスモデルのバージョン1.0は，今後数回にわたり続く改訂作業の出発点となるべきもので，年単位より短い間隔で改訂版を発表してゆくことを目指している。したがって，次のステップとしては，厳密な定義をまとめた章を起草することになっており，UMLを用いた形式化が予定されている。

本論では，インダストリー4.0に関連する他の出典から引用した文章や箇所については，それを明記するように努めた（たとえばVDI/VDE GMA 7.21など）。

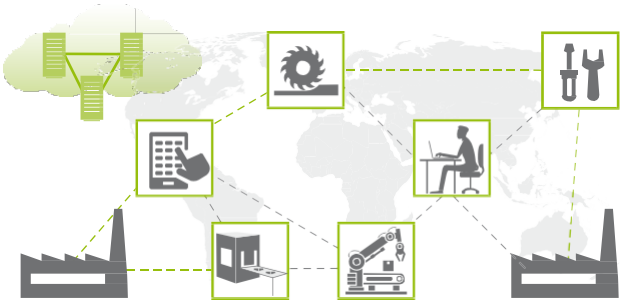
最終的には，術語の用法をGMA 7.21のものと統一することを目指している。また，例についてはそれが例であることを明記し，その中に明記されていない事項が排除されてしまうことを防ぐようにした。

6.3.1 インダストリー4.0に関する議論との位置づけ

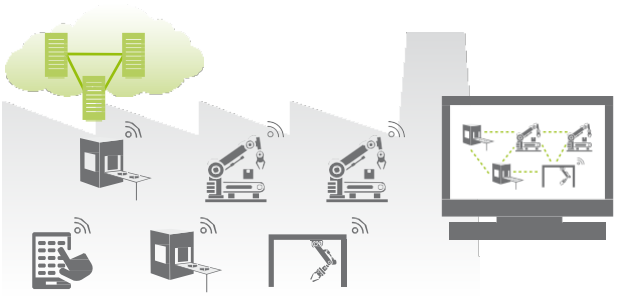
インダストリー4.0の議論は，大まかに言って[3]から転載した下の図にある四つの側面の絡み合いと捉えることができる。

4 出典：IEC 61512, IEC 62264, ISA Draft 88/95 Technical Report, Platform Industrie 4.0

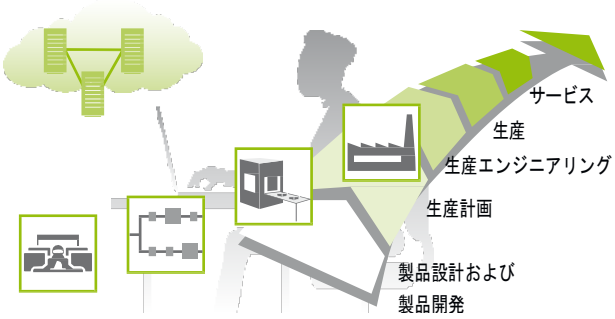
価値ネットワークを横断する水平統合



垂直（統合とネットワーキングされた生産システム）



価値連鎖全体を通じた
エンジニアリングのデジタル一貫性



価値創造の指揮者としての人間

図17：インダストリー4.0の四つの重要な側面[5]

上図によればその四つの側面とは以下のものである：

- インダストリー4.0の側面（1）
  価値ネットワークを横断する水平統合
- インダストリー4.0の側面（2）
  垂直統合，工場や製造工程内など
- インダストリー4.0の側面（3）
  ライフサイクル管理，エンジニアリングの終始一貫性
- インダストリー4.0の側面（4）
  価値ネットワークの指揮者としての人間[6]

本論で解説するインダストリー4.0コンポーネントとは，インダストリー4.0の上記の側面を促進し可能にするデータや機能を記述し提供することができるフレキシブルな枠組を示すものである。

本論記載の各種コンセプトは，現時点においては主に（2）の側面のためのものであり，（3）の側面による要求条件を考慮に入れている。

6.3.2 他の作業部会による関連資料

VDI/VDE GMA 7.21：インダストリー4.0：オブジェクト・エンティティ・コンポーネント

VDI/VDA GMA 7.21による定義については前各章を参照されたい。

タイプとインスタンス

インダストリー4.0におけるタイプとインスタンスの区別に関する技術の現状について簡単に取り上げる。

5 [3]を参考に作成，右下の写真出典：Festo

6 バウエルンハンスル教授による

ライフサイクル

フラウンホーファー研究所IPAのコンスタンティネスキュ教授およびバウエルンハンスル教授によれば，工場運営にあたってさまざまな次元のライフサイクルがインダストリー4.0に関与することになる。

- **製品**：工場では複数の製品を生産する。各製品ごとに独自のライフサイクルがある。
- **オーダー**：製造されるオーダーにはそれぞれのライフサイクルがあり，オーダー実行時にその特異性を生産に反映させることが可能でなければならない。
- **工場**：工場にもライフサイクルがある。工場の資金確保・計画・建設・再利用などである。
  工場は異なる製造者の生産システムや機械を統合する。
- **機械**：機械は発注・設計・コミッショニング・運用・保守・改造・処分などが行われる。
  機械製造者はそのために個々の納入部品を購買するが，本論ではこれをオブジェクトと呼ぶ。納入業者（通常はコンポーネントメーカー）では，その納入部品にもやはりライフサイクルが存在する。
- **コンポーネント**：計画と開発，ラピッドプロトタイピング，設計，生産，使用からサービスまで

図18を見るとこれがよくわかる。

ライフサイクルのつながり

タイプとインスタンスを区別する必要がある理由は，さまざまな取引先があって，それぞれの計画プロセスを伴うライフサイクルが相互に作用するからである。計画段階では，さまざまな仮説や選択肢が検討される。計画では考えられるオブジェクトを想定し，これを「タイプ」と呼ぶ：

図18：インダストリー4.0コンポーネントに関わるライフサイクル[7]

7 出典：マルティン・ハンケル，Bosch Rexroth；トーマス・バウエルンハンスル教授，フラウンホーファー研究所IPA；ヨハネス・ディーマー，Hewlett-Packard

- **納入業者**はこれを「部品タイプ」と呼ぶ。製造とそれに続く顧客（機械製造者）への出荷が行われてはじめてインスタンスが「生成」され，製造者が納入部品として使用する。
- **機械製造者**は顧客と打合せをして「機械タイプ」を計画する。特別な機械の設計および製造によりインスタンスが生成され，それを工場運営者が使用する。
- **工場運営者**は製品の開発にあたって，やはりまず製品タイプを開発する。オーダーがあってはじめて製造が開始され，具体的な製品インスタンスの製造が行われて出荷される。

ここで注目に値するのは，それぞれのタイプを設計・計画する際に，価値ネットワークの下流にある取引先が利用できるような情報やデータが多数生成されるという点である。特定のインスタンスを生産する際にも，さらに新しい情報が加わる（トラッキングデータや品質データなど）。そのため，インダストリー4.0コンポーネントのリファレンスモデルでは，タイプとインスタンスを同等かつ同様に取り扱う。

インダストリー4.0リファレンスアーキテクチャモデル（RAMI4.0）

「インダストリー4.0リファレンスアーキテクチャモデル（RAMI4.0）」の定義については前各章を参照されたい。ここで紹介する「インダストリー4.0コンポーネント」は，RAMI4.0の各層に位置づけられる。ライフサイクルおよびバリューストリームのさまざまな位置や，異なる階層レベルにマッピングする可能性があり，一意的に規定するためには具体的なインスタンス化が必要である。

6.3.3 「インダストリー4.0コンポーネント」

6.3.3.1 本章では初めて一般に認められたインダストリー4.0コンポーネントの定義を導出する。「オフィスフロア」と「ショップフロア」のインダストリー4.0コンポーネントの線引き

責任範囲の線引きを行うために，企業では「オフィスフロア」と「ショップフロア」を区別するのが一般的である。しかし，最近の企業ではこのふたつの領域の絡み合いが次第に強まってきている。自動化技術を中心に考えた場合には，「オフィスフロア」の重要性が薄れる一方で，考慮する必要がある「ショップフロア」の要求が増大する。

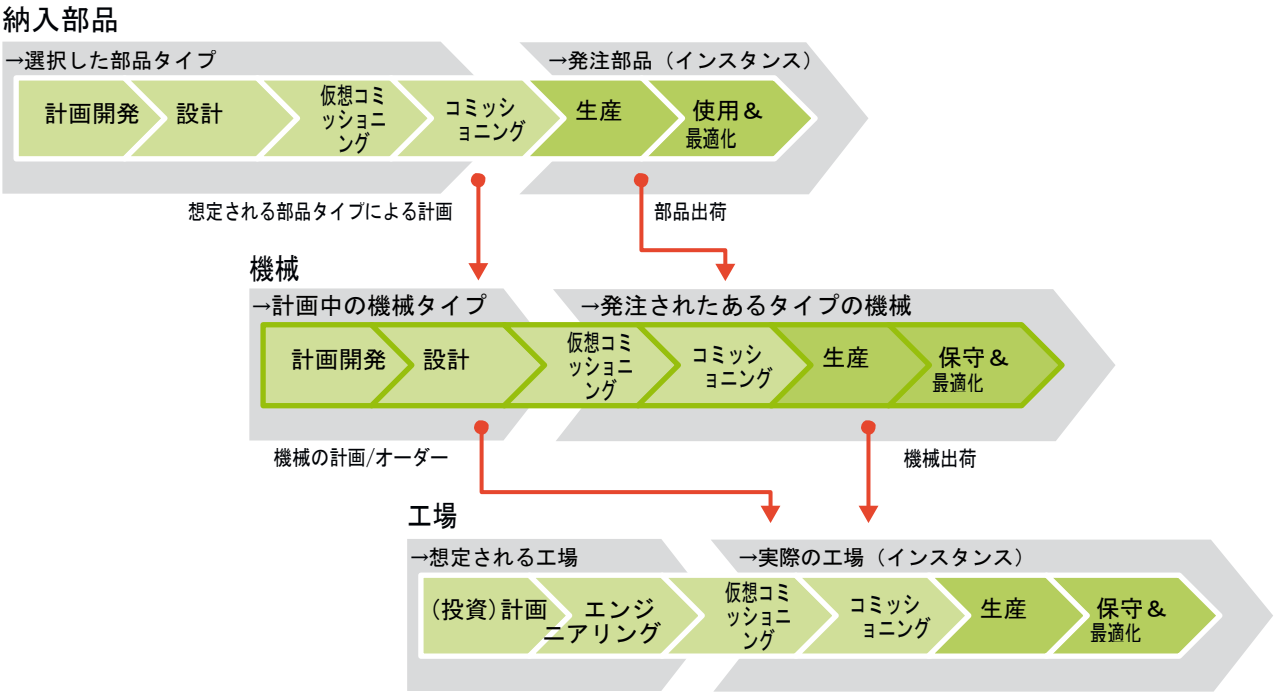


図19：ライフサイクルにおけるタイプとインスタンス

同じことが逆方向にもいえる。下図にある任意の終点との接続性および共通セマンティックモデルという要求を踏まえ，コンポーネントはレベルに依存しない共通の特性を有していなくてはならない。その内容はインダストリー4.0コンポーネントの形式の中で規定されている。

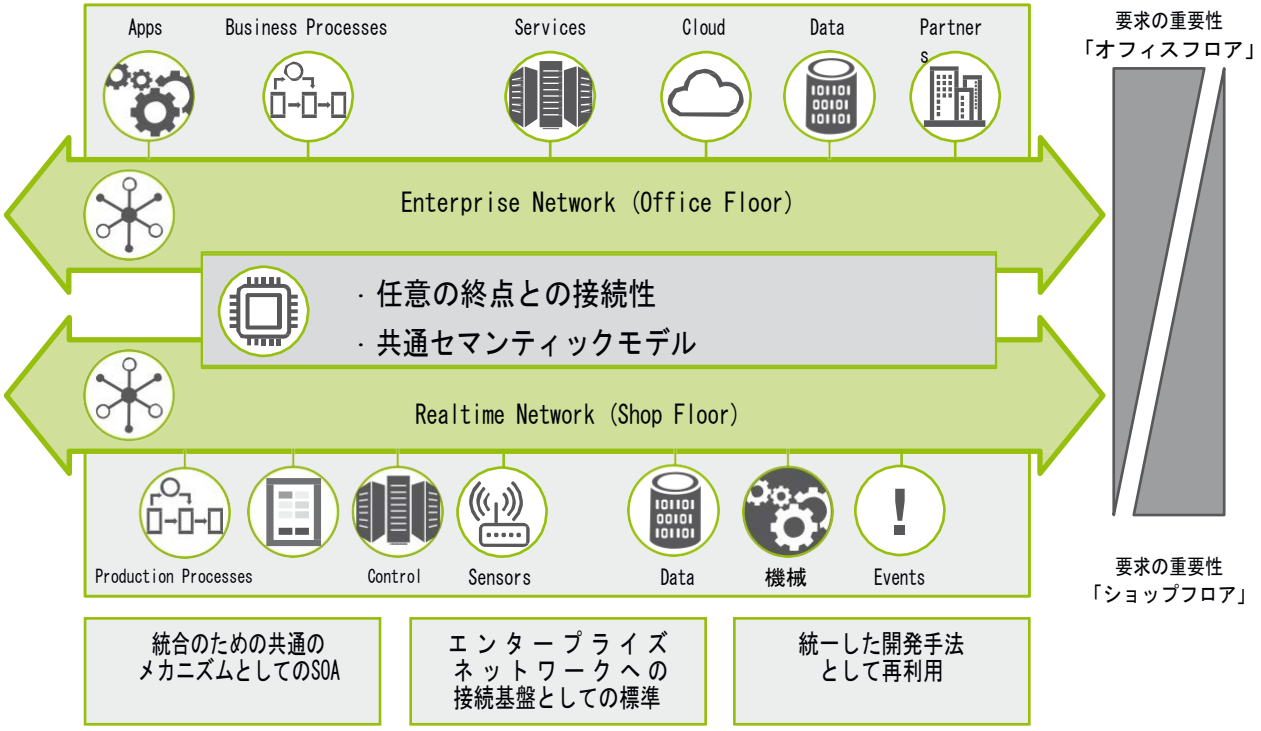


図20：「オフィスフロア」と「ショップフロア」の線引き

インダストリー4.0コンポーネントは，ひとつの生産システムや個別の機械やステーション，また一台の機械内にあるユニットなども表すことができる。したがってインダストリー4.0コンポーネントは（その種類こそさまざまなものがあるが）いずれも「オフィスフロア」と「ショップフロア」の間で重要性を巡る駆け引きが行われる微妙な位置にあり，工場のライフサイクルに沿って，PLM（製品ライフサイクル管理）やERP（企業資源計画），工業用制御システム，物流システムなどといった中心的かつ重要な工場システムと接する形で動作する。

要求条件：
インダストリー4.0コンポーネントのネットワークは，任意の終点（インダストリー4.0コンポーネント）の間での接続が可能なように構成されていなければならない。インダストリー4.0コンポーネントおよびその内容は共通のセマンティックモデルに沿ったものでなければならない。

要求条件：
インダストリー4.0コンポーネントのコンセプトは，重点の異なる要求条件（すなわち「オフィスフロア」または「ショップフロア」）にも対応できるような差別化を行うことが可能でなくてはならない。

6.3.3.2 オブジェクトからインダストリー4.0コンポーネントへ

次に，GMAが行った個々の規定を相互に関連づけることでインダストリー4.0コンポーネントの定義を見出すことにする。

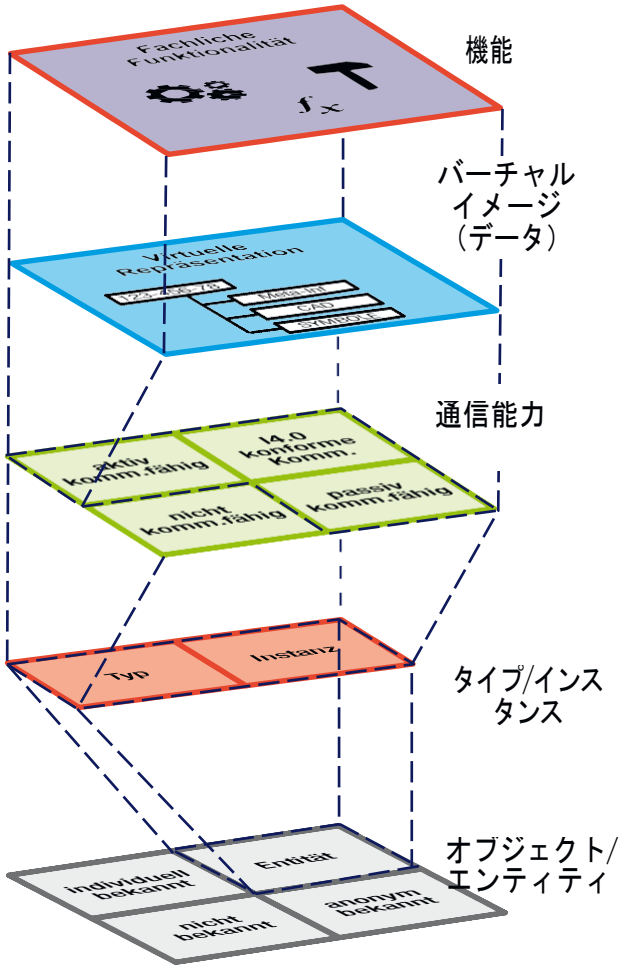


図21：GMA 7.21によるインダストリー4.0コンポーネントの層構造

オブジェクトクラス：

- GMAは四通りのオブジェクトクラスを規定している：
- 未知
- 匿名既知
- 識別既知
- エンティティ

データや機能をひとつのオブジェクトに結びつけるためには，オブジェクトがエンティティとして存在する必要がある。従来の意味において物理的および非物理的な出荷がいずれも考えられるソフトウェアもやはりオブジェクトである。アイデアやアーカイブ，コンセプトなどもこの意味ではオブジェクトである。

備考1：
データおよび機能を情報システムで提供することがインダストリー4.0コンポーネントの目的のひとつであるので，GMAの定義による識別既知オブジェクトは，おのずとエンティティに移行することになる。

備考2：
以下，オブジェクト/エンティティを指す場合には，常にオブジェクトという。

タイプ/インスタンス

オブジェクトはタイプまたはインスタンスとして既知である可能性がある。タイプとしてオブジェクトが既知であるのは，たとえば計画段階においてである。計画中のオブジェクトの注文情報が既知であれば，そのオブジェクトを識別既知タイプとみなすことができる。インスタンスとみなされるのは，たとえば現実に存在する機械のオブジェクトなどである。ひとつのタイプを繰り返しインスタンス化することによる可算性という意味におけるみせかけのインスタンス（ロット）については現時点では別途考慮していない。ここではインスタンス化の具体的な実行と，基となるタイプとの関連付けを前提とすべきである。

通信能力

インダストリー4.0コンポーネントの特性を提供できるようにするには，オブジェクトと接続された情報システムが少なくともひとつ必要である。そのため，オブジェクトに少なくとも受動的な通信能力が備えられていることが前提となり，これはすなわち，GMA専門委員会7.21が規定したインダストリー4.0対応通信能力は必ずしもオブジェクトには必要ないことを意味する。よって既存のオブジェクトをインダストリー4.0コンポーネントとして「拡張」することが可能となる。この場合，上位のITシステムがインダストリー4.0対応通信の一部をSOAアーキテクチャおよびプロキシの原理によって担当することになる。

そうすることでたとえば識別可能な端子台やProfiNetデバイス（I&Mデータを通じて識別可能）などもインダストリー4.0コンポーネントになる可能性がある。

バーチャルイメージ

バーチャルイメージにはオブジェクトに関するデータが保持される。このデータはインダストリー4.0コンポーネント自身の「上/内」に保持されて，インダストリー4.0対応通信を通じて外界に提供することもできる。もしくは，（上位）ITシステム上に保持して，このシステムがインダストリー4.0対応通信によってデータを外界に提供する。

リファレンスアーキテクチャモデルRAMI4.0では，バーチャルイメージは情報層にある。したがってインダストリー4.0対応通信の持つ意味合いが大きくなる。

要求条件：
インダストリー4.0対応通信は，インダストリー4.0コンポーネントのバーチャルイメージデータを，オブジェクト自体の中か，（上位）ITシステムに保持することができるような仕様でなければならない。

バーチャルイメージで重要なのが「マニフェスト」[8]であり，これはバーチャルイメージの個々のデータ内容の目録と考えることができる。すなわちその中にはいわゆるメタ情報が含まれている。また，インダストリー4.0コンポーネントに関する必須事項も含まれており，たとえば適切な識別方法によるオブジェクトとの接続にあたって必要となる。

バーチャルイメージに含まれるそれ以外のデータとしては，ライフサイクルの個々の段階に関するデータで，CADデータや接続図，ハンドブックなどが考えられる。

専門機能

インダストリー4.0コンポーネントは，データに加えて専門機能を有する可能性もある。このような機能としてはたとえば次のようなものが考えられる：

- オブジェクトに関連する「ローカルプランニング」用ソフトウェア。例：溶接計画，端子台の印字用ソフトウェアなど。
- プロジェクト設計・コンフィグレーション・操作・保守用のソフトウェア
- オブジェクトに対する付加価値
- ビジネスロジック実行のために重要なその他の専門機能

リファレンスアーキテクチャモデルRAMI4.0では，専門機能は機能層にある。

6.3.3.3 「管理シェル」によってオブジェクトがインダストリー4.0コンポーネントになる

前項で述べたように，通信能力の異なるさまざまなオブジェクトをインダストリー4.0コンポーネントの仕様とすることができる。本項ではそのさまざまな仕様形態について，例に則してより詳細な検討を行う。インダストリー4.0コンポーネントのコンセプトにおいては，このような仕様形態はいずれも同等のものである。

図22からは，オブジェクトがどのような種類のものでも，最初からインダストリー4.0コンポーネントではないことがわかる。エンティティであって少なくとも受動的な通信能力をもつことが前提のオブジェクトが「管理シェル」に包まれてはじめて，インダストリー4.0コンポーネントと呼べるようになる。

前項で述べたオブジェクトのバーチャルイメージと専門機能がこの管理シェルに含まれることになる。

8 JARファイルのために選択，マニフェスト[11]参照

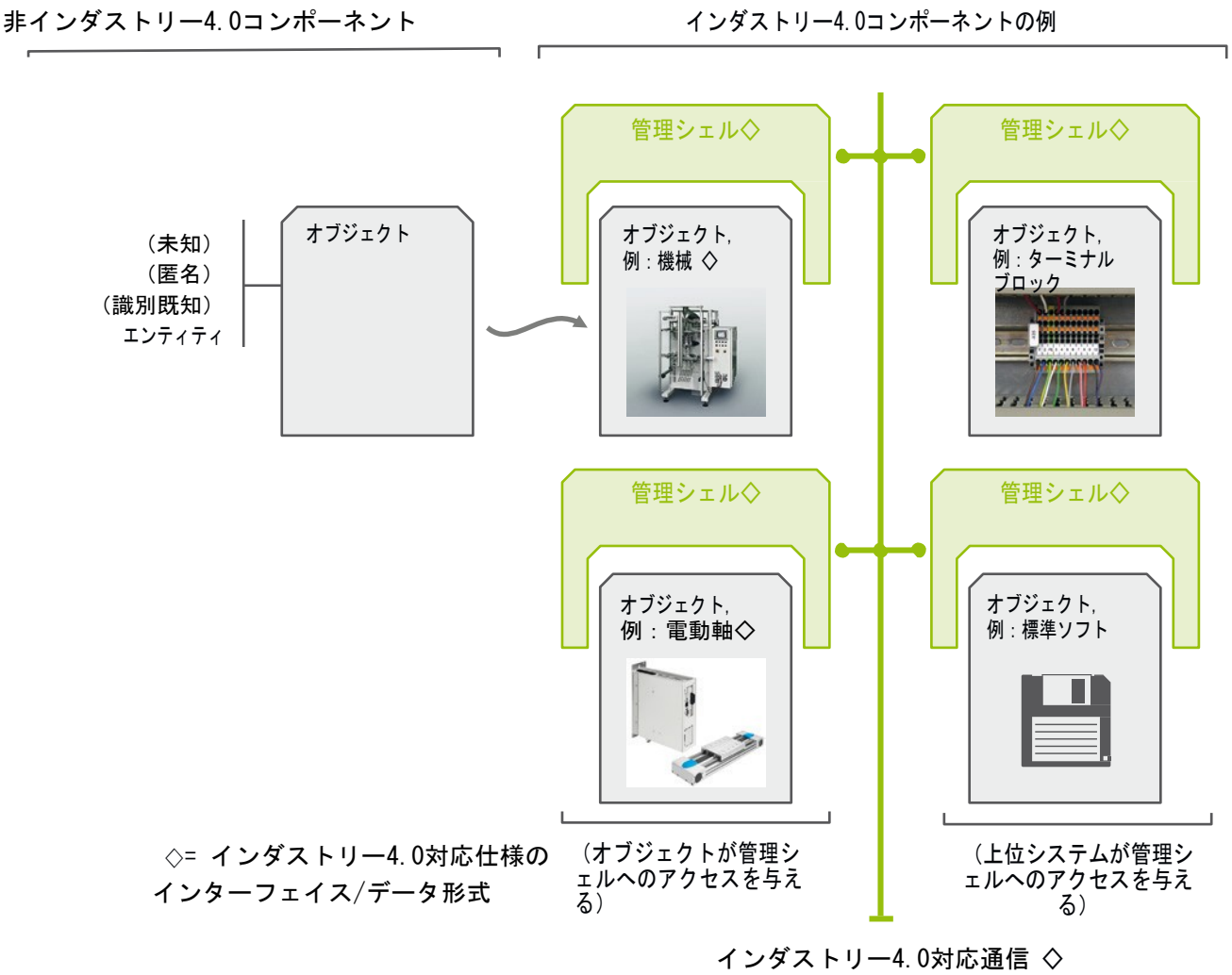


図22：オブジェクトからインダストリー4.0コンポーネントへ

上図には考え得るオブジェクトとして四つの例が記載されている：

1. 機械全体の場合には，なによりも制御系を有していることから，インダストリー4.0コンポーネントの仕様とすることが可能である。この場合にインダストリー4.0コンポーネントの仕様にする役割はたとえば機械製造者が受け持つことになる。

2. 納入業者による戦略的に重要なユニット[9]なども独立したインダストリー4.0コンポーネントとみなし，たとえばアセットマネジメントシステムや保守システムなどで単独に扱うことができる。インダストリー4.0コンポーネントの仕様にする役割はたとえばコンポーネント製造者が受け持つことになる。

9 コンポーネントという言葉を避けるため

3. 同様に機械の個々の設計ユニットもインダストリー4.0コンポーネントとみなすことができる。たとえばターミナルブロックにとって重要なのは，各信号の結線状態を記録し，機械のライフサイクルを通じて更新してゆくことである。この場合にインダストリー4.0コンポーネントの仕様にする役割はたとえば電気設計者や電気工が受け持つことになる。

4. さらに，提供されたソフトウェアが生産システムの重要なアセットであり，よってインダストリー4.0コンポーネントとなる可能性もある。

このような標準ソフトウェアとして考えられるのはたとえば独立した計画ツールやエンジニアリングツールなどで，製造の操業に現在重要であるか，将来重要となるものである。また，納入業者が自らの製品の拡張機能を提供するライブラリを純粋なソフトウェアとして販売しようとすることも考えられる。この場合にインダストリー4.0コンポーネントの仕様にする役割はたとえばソフトウェアの提供者が受け持つことになり，IEC61131準拠の各コントローラへの分配は複数のインダストリー4.0システムによって行われる。

図22は，論理ビューとして，オブジェクトには「管理シェル」がつきものであることを表したものである。配置ビューでは，オブジェクトと管理シェルが離れた状態で存在することも十分に考えられる。たとえば，受動的な通信能力を有するオブジェクトで，管理シェルが上位ITシステムにマッピングされる[10]場合もある。オブジェクトの受動的な通信能力と上位ITシステムのインダストリー4.0対応通信によって，オブジェクトと管理シェルの接続が確保される。オブジェクトに能動的な通信能力があるが，インダストリー4.0対応の通信はできない場合も同様である。インダストリー4.0対応の通信能力がある場合にのみ，管理シェルをオブジェクト「内」にマッピングすることができる（たとえば機械のコントローラに格納されてネットワークインターフェイスを通じて提供される）。インダストリー4.0コンポーネントのコンセプトにおいては，すべての選択肢を同等とみなす。

ひとつのオブジェクトに目的の異なる複数の管理シェルがある場合もある。

要求条件：

上位ITシステムが管理シェルをインダストリー4.0対応の形で提供する方法（SOAの手法，プロキシの原理）を適切なリファレンスモデルによって記述する必要がある。

10 「ホストされて」

要求条件：

管理シェルを製造者（コンポーネント製造者，電気設計者など）から上位ITシステムに「搬送」する方法（たとえばEメールに添付するなど）を記述する必要がある。

6.3.3.4 さらなる用語の線引き

下図は各用語の線引きをさらに明確に示したものである。

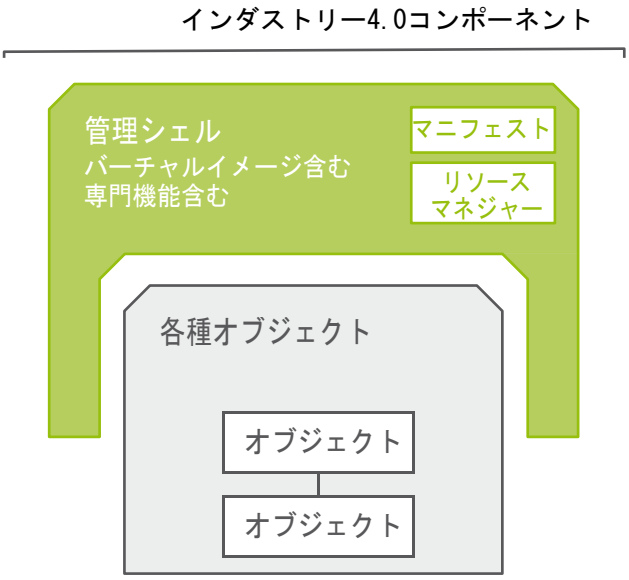


図23：インダストリー4.0コンポーネント

論理ビューにおいて，インダストリー4.0コンポーネントには単数ないし複数のオブジェクトとひとつの管理シェルが含まれ，この管理シェルにバーチャルイメージおよび専門機能のデータが入っている。マニフェストはバーチャルイメージの一部としてインダストリー4.0コンポーネントの管理に必要な項目を詳述したものである。GMA専門委員会7.21の定義によれば，「リソースマネジャー」も管理シェルの一部である。よってITの各種サービスが管理シェルのデータや機能にアクセスし，外部に提供できるようになっている。

管理シェルおよびその管理オブジェクトは，いずれかのオブジェクトの「エンベデッドシステム」内に「ホスト」されていたり（能動的インダストリー4.0対応通信能力），単数または複数の上位ITシステムに配置されている（配置ビュー）可能性がある。

要求条件：
上位システムの種類によっては，管理オブジェクトを複数の上位ITシステムに配置する可能性が必要となる。

サイバーフィジカルシステム

インダストリー4.0コンポーネントはサイバーフィジカルシステムを特化させたものといえる。

6.3.3.5　配置ビューから見たインダストリー4.0コンポーネント

前項では，論理ビューから見た場合，インダストリー4.0コンポーネントでは，どのオブジェクトにも必ず「管理シェル」がつきものであることを解説した。しかし，配置ビューでは状況に応じて管理シェルを上位システムに配置することが可能であることも述べた。

インダストリー4.0コンポーネントをリポジトリにマッピング

わかりやすいように，「デジタルファクトリー」のリポジトリに対応した図として表すこともでき，これは上述の各種コンセプトに一致するものである。

インダストリー4.0コンポーネントをオブジェクトによりマッピング

インダストリー4.0コンポーネントのオブジェクトがインダストリー4.0対応の通信能力（[2]記載のCP34またはCP44）を有している場合には，インダストリー4.0コンポーネントをオブジェクトによってマッピングすることもできる。

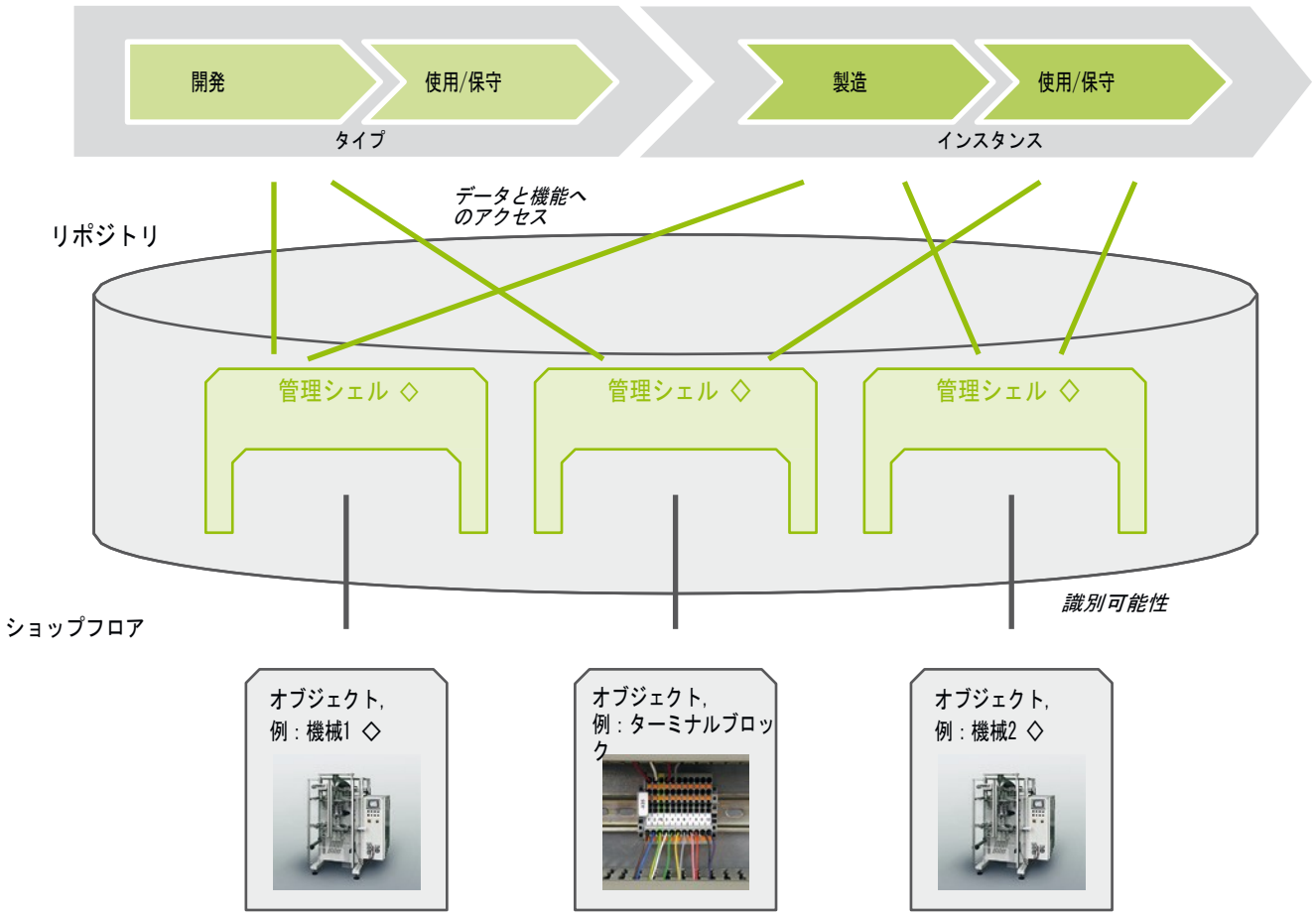


図24：リポジトリ

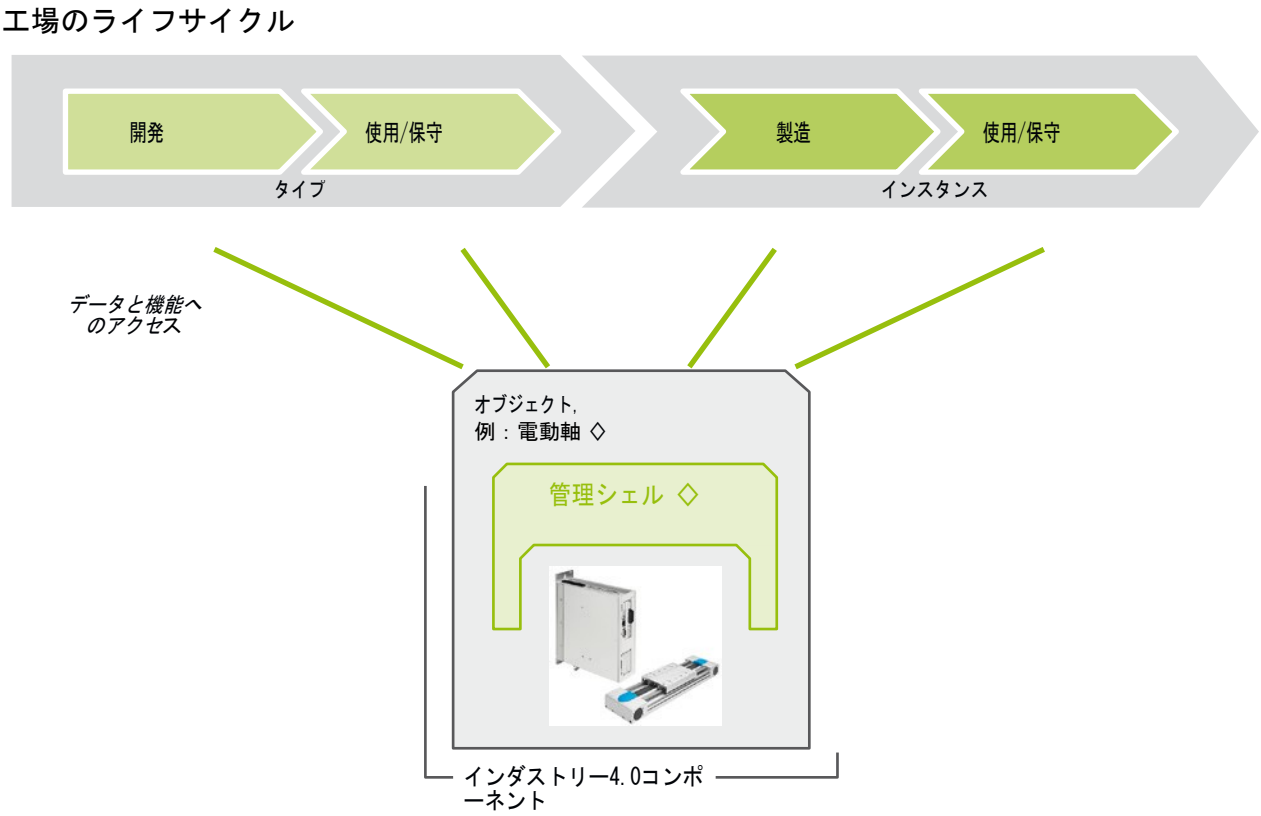


図25：工場のライフサイクル

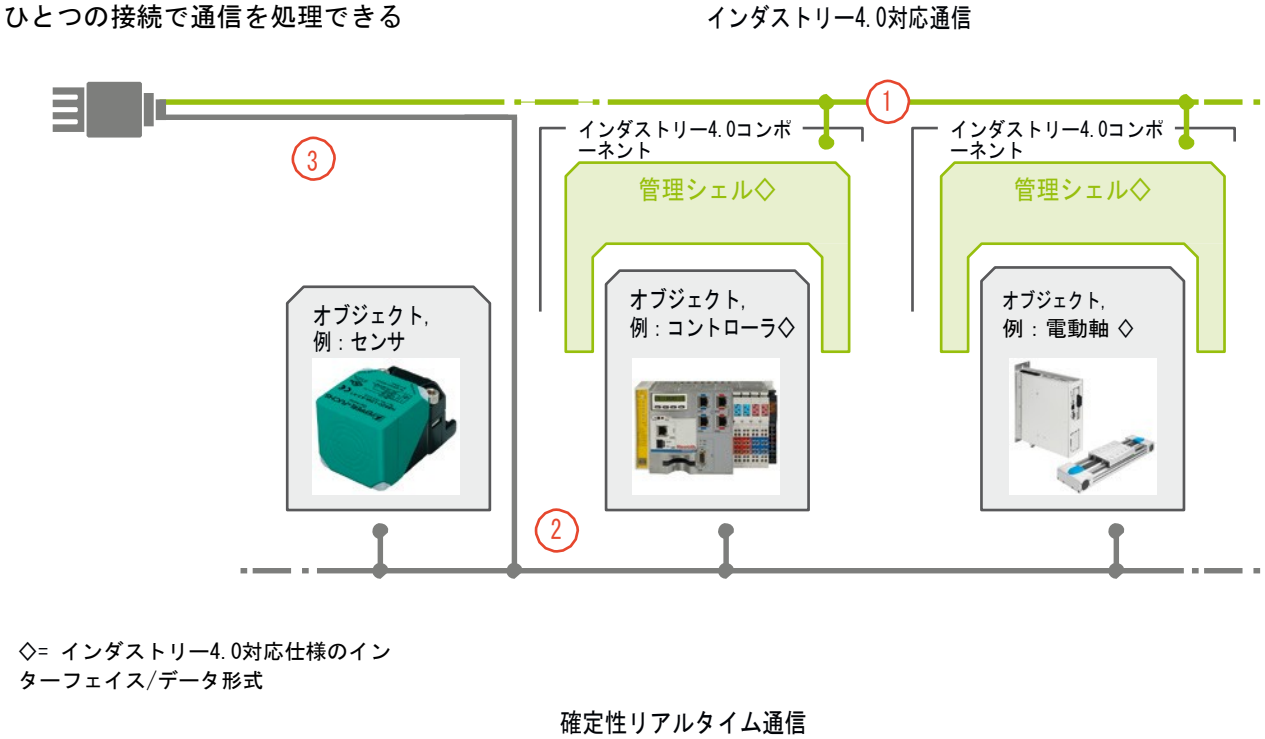


図26：インダストリー4.0コンポーネントのカプセル化能力とネットワーキング

インダストリー4.0コンポーネントのカプセル化能力

インダストリー4.0コンポーネントは，インダストリー4.0工業内の考え得るあらゆる接続に対応することが明確に意図されている（図？）。しかしこのようなネットワーキングが主要機能を制約することがあってはならない（図？）。「外部の」ネットワークに不具合があってもこの主要な領域を支障なく維持することができる能力を，SG2（ZVEI組織内ミラー委員会リファレンスアーキテクチャ）およびSG4（ZVEI組織内ミラー委員会セキュリティ）は「カプセル化能力」と呼んでいる。

要求条件：
インダストリー4.0コンポーネントは，特に管理シェルとそれに含まれる機能およびそのためのプロトコルなどについて「カプセル化能力」を有していなければならない。

本コンセプトではこの要求を満たすために，独立したデータオブジェクトないし機能オブジェクトとして管理シェルを設計している。その中に含まれるデータや機能へのアクセスは「関心の分離（SoC）[11]」の原理に基づいて構成し，製造にとって決定的な重要性をもつプロセスに影響が及ぶ可能性を現在の技術において排除できるようにする。

この原理を採用することで，現在の技術では製造において使用されているイーサネットベースのフィールドバスを完全にインダストリー4.0対応通信に置き換える必要がなくなる（移行シナリオ）。

ただし，インダストリー4.0対応通信と確定性ないしリアルタイムの通信の間には相互の調整が必要で，たとえば可能な限り同じ（物理）インターフェイスおよびインフラを使用する。ふたつの通信チャネル間で矛盾が生じないように確実に対処する必要がある。

本論で解説したリファレンスモデルにとってこのような議論が意味するところは，確定性ないしリアルタイムの通信の特性すべてをインダストリー4.0対応通信自体が実装する必要はく，既存の技術に肩代わりしてもらうことができるということである。

要求条件：
インダストリー4.0コンポーネントの目的は，オブジェクトシェルに出入りするインダストリー4.0非対応の通信接続を掌握し，終始一貫性のあるエンジニアリングを可能にすることである。

現在一般的に使用されているリアルタイムイーサネットプロトコルを見る限り，同じ通信インフラ（差し込み口，プラグ，中継器）を使って二種類の通信を処理することが可能と思われる（図26③）。「関心の分離」の原理によれば，二種類の通信はロジックでは分離されたままである。

ひとつのインダストリー4.0コンポーネントに複数のオブジェクトが含まれている可能性がある

本項では，インダストリー4.0コンポーネントに含まれるオブジェクトはひとつとは限らず，複数ある可能性もあることを例に即して説明する。

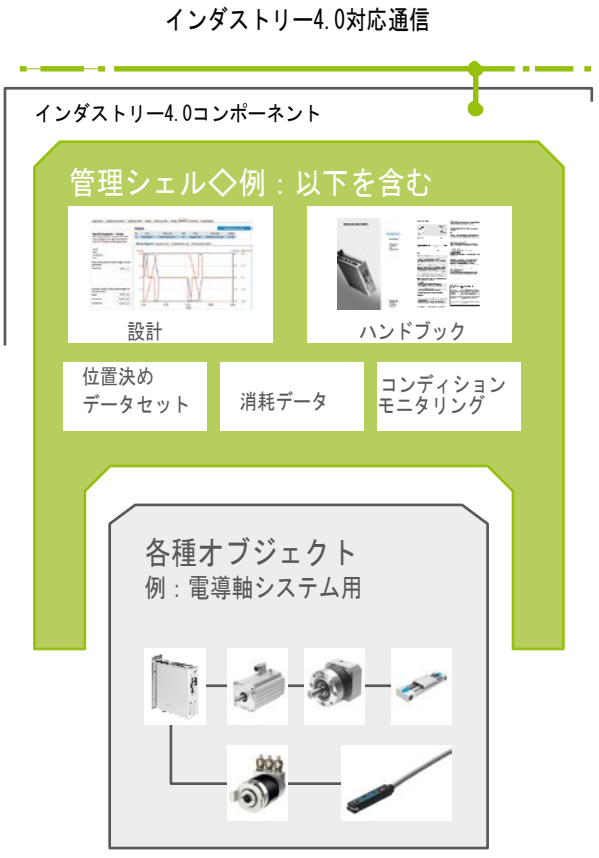


図27：複数のオブジェクトで構成されるインダストリー4.0コンポーネント

11 http://en.wikipedia.org/wiki/Separation_of_concerns

図27は，複数のオブジェクトがまとまってひとつの電導軸システムを形成する例を示している。ある製造者の設計ソフトウェアによって，エンジニアリングの段階で，個々のサブシステムがひとつのシステムとして組み上げられたものである。さらにコンフィグレーションソフトウェアがあり，これを使ってシステム全体を稼働させることができる。位置決めデータセット，記録された消耗データ，コンディションモニタリングなどは，システムの各構成要素の相互関係を確立する（最大動作長などに関して）ために必要となる。

したがって，これらのオブジェクトをひとつのシステムとして管理し，インダストリー4.0コンポーネントとしてマッピングしたほうがインダストリー4.0の観点からは有意義である。

これをインダストリー4.0コンポーネントとしてひとつひとつ分解したとすると，多数の意味合いの異なる相関関係を単数ないし複数の上位インダストリー4.0システムによってマッピングする必要が生じ，無用な複雑化を招くことになろう。

6.3.3.8 ひとつのインダストリー4.0コンポーネントはロジックの入れ子が可能な場合がある

インダストリー4.0の側面（2）「垂直統合」の中で，オーダーに合わせて（企業）アセット[12]を設定しなおしたり，再利用したりするために，生産システムのモジュール化をインダストリー4.0は要求している。つまり，ひとつのインダストリー4.0コンポーネントがロジックにおいて他のコンポーネントも包括し一体化して動作し，上位システムに対してロジック上抽象化するという可能性がこのコンセプトでは想定されている。

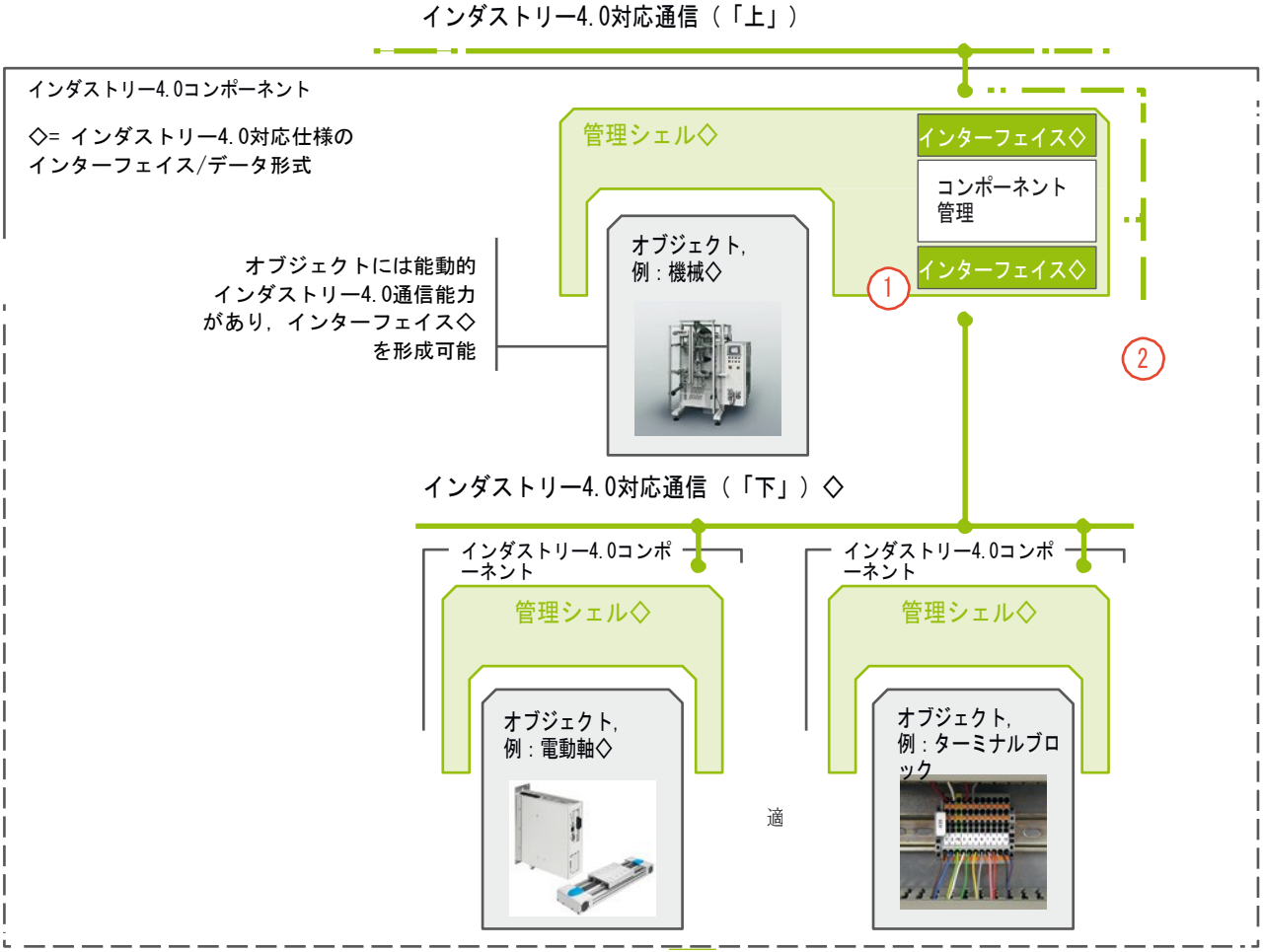


図28：インダストリー4.0コンポーネントの入れ子可能性

12 [3]参照：「また，適切な知的装置の能力記述とも併せ，生産システムのアドホックネットワークや再設定を可能とするための前提となるモジュール化および再利用のコンセプトを作成する必要がある。」

さらに，インダストリー4.0の側面 (3) 「エンジニアリングにおける終始一貫性」では，ひとつの生産システムに属するできる限り多数のオブジェクトについて，より踏み込んだデータやエンジニアリング内容などをオンラインで利用可能とすることが求められている。管理シェルでは，インダストリー4.0コンポーネントのオブジェクトに一意的に関連付けることのできるデータは，それに応じて分散した形で利用可能であることが想定されている。そのような形で分散したデータは，分散型エンジニアリングや迅速な再設定を行うのに好都合である。

したがって，インダストリー4.0コンポーネントのコンセプトは，ひとつのインダストリー4.0コンポーネント（機械全体など）に他のインダストリー4.0コンポーネントをロジック上割り当てることで（一時的な）入れ子状態となることを想定すべきである。

技術的には，上位オブジェクト（機械など）がインダストリー4.0対応の通信インターフェイスをふたつ形成することで，ロジック上および物理的にも上位と下位のインダストリー4.0コンポーネントを明確に分離するような仕様（図中①）が考えられる。また別の可能性としては，「上」と「下」のインダストリー4.0対応通信が物理的にはひとつであるが，ロジックでは分離される方法（図中②）がある。

このような「下位」インダストリー4.0コンポーネントの論理割当を管理するために，管理シェルに適切な「コンポーネント管理」を設けることも可能である。これがたとえば機械の再設定を助けたり，機械の状態を「上に向かって」適切に表現することも考えられる。

要求条件：
ひとつのインダストリー4.0コンポーネント（機械全体など）に他のインダストリー4.0コンポーネントをロジック上割り当てることで（一時的な）入れ子状態となるようにする。

要求条件：
上位システムには，その目的に応じ，かつ制限可能な形で，（一時的に）ロジック上割り当てられているコンポーネントも含め，すべてのインダストリー4.0コンポーネントへのアクセスを可能にする必要がある。

6.3.3.9 状態モデル

インダストリー4.0コンポーネントの状態は，インダストリー4.0対応通信の他の参加端末から常に呼出可能である。これは定義された状態モデルに基づくものである。

インダストリー4.0コンポーネントは階層構造をなす可能性があるので，ひとつの状態における下位の状態を適切に表現する方法（機械の一部が運転可能な状態でない場合に，それが機械にどのような意味をもつか）を定義することが望ましい。

それに加えて，バーチャルイメージおよび専門機能の状態について詳細なビューが可能となるような多数の状態変数を状態モデルに備えさせるべきである。これにより，ある時点tにおけるインダストリー4.0コンポーネントの状態のビューの整合性をとることができ，統計的に適正なデータ解析などに利用できる。

6.3.3.10 インダストリー4.0コンポーネントの一般的プロパティ

GMA 7.21[2]では，インダストリー4.0の文脈におけるコンポーネントという用語を以下のように定義している：

コンポーネントという用語は広義である。物理世界および情報世界のオブジェクトで，そのシステム環境において特定の役割を果たすか，そのために設けられているものを指す。コンポーネントは，たとえばパイプであったり，PLCのファンクションブロックであったり，ランプやバルブ，知的駆動ユニットだったりする。重要なのは，一体として捉えることと，あるシステムの中で果たすべき，ないし既に果たしている役割（機能）との関係である。インダストリー4.0コンポーネントと我々が呼ぶのは，特殊なコンポーネントである。インダストリー4.0コンポーネントの特徴は，上述したクラシフィケーションのプロパティに関して特定の要求条件を満たしている点にある。インダストリー4.0システム内にも，この要求条件を満たしていないコンポーネントが多数あるが，このようなコンポーネントはしたがってインダストリー4.0コンポーネントではない。

このコンセプトでは，受動的または能動的な通信能力はあるものの，インダストリー4.0対応通信能力はないオブジェクトも含まれる可能性がある。このため，本書でいうインダストリー4.0コンポーネントとは以下のようなものである：

- CPクラシフィケーションではCP24，CP34，CP44のコンポーネントであること。
- インダストリー4.0ネットワークにおける完全なサービスシステム参加端末となるような通信が可能な管理シェルを有していること。

次の項はGMAによる定義[2]を基に手を加えたもので，各コンセプトをさらに詳細に説明している。これは[2]と完全に一致するものだが，インダストリー4.0ネットワークのサービスシステム参加端末としてのインダストリー4.0コンポーネントに要求されているのは以下のプロパティである（要求条件）：

識別可能性

ネットワーク内で一意的に識別可能であり，その各物理オブジェクトはそれぞれ一意的な識別子（ID）によって識別される。CP34またはCP44のコンポーネントである場合には，通信アドレス（IPアドレス等）によってアクセス可能である。

インダストリー4.0対応通信

インダストリー4.0コンポーネント同士は少なくともSOA原理（共通のインダストリー4.0対応セマンティックスを含む）に基づいて通信する。

インダストリー4.0対応のサービスおよび状態

インダストリー4.0システム全体で標準化された（追加組み込みも可能な）サービス機能および状態をサポートする。

仮想記述

自らの動的挙動も含めた仮想記述を提供する。この記述はバーチャルイメージとマニフェストによって達成される。

インダストリー4.0対応セマンティックス

インダストリー4.0システムで標準化されたインダストリー4.0対応セマンティックスをサポートする。

セキュリティとセーフティ

自らの機能およびデータに対し，タスク相応の保護を提供する（セキュリティ）。その他にもアプリケーションにおいて機能的安全性や機械安全性のための対策が必要になる可能性がある（セーフティ）。

クオリティオブサービス

そのタスクに必要な特性をクオリティオブサービス（QoS）として有していること。自動化技術系アプリケーションの場合には，リアルタイム能力やフェイルセーフ性，時計同期などがそのような特性にあたる。これらの特性は，プロファイルに基づくものであることが考えられる。

状態

常に自らの状態を通知すること。

入れ子可能性

インダストリー4.0コンポーネントはどれも複数のインダストリー4.0コンポーネントにより構成される可能性がある。

本書の文脈におけるインダストリー4.0コンポーネントとは，生産システム，機械，ステーション，設計上重要な機械部品および機械ユニットなどを指す。

プロパティ（1）について：識別可能性

インダストリー4.0方式の目的は，すべての関連データにリアルタイムでアクセス可能とすることである。インダストリー4.0コンポーネントは，現在のインフラを拡張するための重要な要素となる。これは生産システムの寿命を通じていえることである。すなわちインダストリー4.0コンポーネントはインダストリー4.0のあらゆる価値連鎖[1]および価値創造プロセスにおいて，終始一貫かつ統一された情報交換を行うために決定的な役割を果たす。

能動的なインダストリー4.0コンポーネントであればインダストリー4.0対応通信を自ら行い，受動的なインダストリー4.0コンポーネントの場合にはそのためのインフラが必要となる。

産業の要求に対応できる通信が必要である。生産システムは常に連携して動作し，遠隔地を結ぶ必要もあることから，広域ネットワーク技術を用いたローカルネットワーク同士の接続の重要性が増している。

要求条件：

インダストリー4.0コンポーネントのネットワーキングでは，ローカルネットワークが広域ネットワーク接続を通じてほぼ制約なしに相互に通信できるような広域ネットワーク技術の挙動が望ましい。

これは該当する接続の可用性および安全性（セキュリティ）に関連する内容だが，即時性についてもいえることである。ストリーミング技術をはじめとするさまざまな仕組みが適切なソリューションの基盤となる可能性はあるものの，この点についてはまだ基本的な研究が必要である。

さらに上のレベルでは，通信の信頼性と長時間にわたる安定性が保証できるような接続が要求される。これに関しては，インダストリー4.0アプリケーションにおける既存のプロトコルの有用性を検討する必要がある。インダストリー4.0コンポーネントへのアドレスと，インダストリー4.0コンポーネントの（アプリケーション）オブジェクトへのアドレスを区別する必要がある。後者は世界共通で製造者横断的に一意的なIDによってアドレスされる。IDの取り扱いについては[4]および[5]ならびにその他の各種標準を参照されたい。

要求条件：

インダストリー4.0コンポーネントへのアドレスと，インダストリー4.0コンポーネントの（アプリケーション）オブジェクトへのアドレスを区別する必要がある。

プロパティ（2）について：
インダストリー4.0対応通信

インダストリー4.0コンポーネントの自己情報は，サービス指向アーキテクチャ（SOA）を基盤としてサービスモデルに基づくサービスによって実現される（リソースマネジャー）。インダストリー4.0コンポーネントのプロファイルを適宜用意することによって，該当するサービスを技術的に実現する方法を制御することができる（たとえばOPC-UA基本サービスなどにより）。

プロパティ（3）について：
インダストリー4.0対応のサービスおよび状態

ショップフロアとオフィスフロアでは異なるアプリケーションに対応する必要があるので，インダストリー4.0コンポーネントでは，アプリケーションレベルによって異なるプロトコルを使用するという選択肢を用意する必要がある。

要求条件：

よってプロトコルやアプリケーション機能はオプションとして追加組み込み可能にする。

プロパティ（4）について：仮想記述

関連性のある動的挙動も含むインダストリー4.0コンポーネントの特性記述用の情報は，現実のコンポーネントのバーチャルイメージからインダストリー4.0データ形式で生成される。このバーチャルイメージの一部をなすのがマニフェストであり，マニフェストには一意的なセマンティックスが要求される。また各種プロパティの仕様も重要である。

マニフェストにはたとえば以下の項目が含まれる：

- 現実のコンポーネントの特徴的プロパティ
- 各プロパティの関係についての情報
- 生産および生産プロセスに関わるインダストリー4.0コンポーネント同士の関係
- 機械の該当する機能とそのプロセスの形式仕様記述

バーチャルイメージにはたとえば以下の項目が含まれる：

- 商業データ
- 履歴データ，たとえばサービス履歴など
- その他・・・

具体的な意味でのマニフェストと一般的な意味での管理オブジェクトとの違いは，マニフェストにはインダストリー4.0の各側面を備えたインダストリー4.0対応ネットワーク実現のため一意的なセマンティックスに従って公開されていなくてはならない情報が含まれているという点である。管理オブジェクトには，製造者自身がどのような形で開示するかを決めることのできる情報が含まれていてもよい。

プロパティ（5）について：インダストリー4.0対応セマンティックス

ふたつ以上のインダストリー4.0コンポーネントの間の情報交換には一意的なセマンティックスが必要である。このセマンティックスは，4記載の特性を用いて，インダストリー4.0全体で共通に規定する必要がある。[4]を見たところ以下の項目によるプロパティのクラシフィケーションが役に立ちそうである：

- 機械構造
- 機能
- 場所
- 生産性
- 事業環境条件

プロパティの取り扱いについては[4]，[5]，[6]を参照されたい。

プロパティ（6）について：セキュリティとセーフティ

インダストリー4.0コンポーネントには必ず，セキュリティ機能を確保するために最低限のインフラが備えられている。それぞれの生産プロセスをセキュリティ分析に直接取り込んではじめてセキュリティは確保されるのであるから，インダストリー4.0コンポーネントに備えられたセキュリティインフラは必要不可欠なものとはいえ，十分なセキュリティ機能を提供するものとはとてもいえない。機能的安全性や機械安全性（セーフティ）を確保する必要がある場合には，各インダストリー4.0コンポーネントの特性にも影響が及ぶ。掌握して評価し，上位システムに送る必要のあるプロパティが増えることになる。

要求条件：

最低限備えられたインフラがセキュリティバイデザイン（SbD）の原則を満たしていなければならない。

プロパティ（7）について：クオリティオブサービス

インダストリー4.0コンポーネントを使用する特定の環境によってその要求条件が決まる。したがってそれぞれの環境で要求される特性（QoS）は，機械や装置に使用するコンポーネントを選択する時点ですでに考慮する必要がある。自動化環境についていえば，その特性とはたとえば：

- 生産的通信用のリアルタイムデッドライン，D1msのリアルタイム対応確定性など
- ネットワークインフラ環境の最高水準のフェイルセーフ性（堅牢性）
- 時計同期
- 相互運用性
- 統一規則に基づく診断とエンジニアリング
- アドホック接続の確立

プロパティ（8）について：状態

インダストリー4.0コンポーネントはどれも，特定のタスクを遂行するための連携体制に加わっており，そのタスク遂行にはプロセスの調整が必要であることから，各インダストリー4.0コンポーネントの状態はいつでもインダストリー4.0対応通信ネットワークの他の参加端末から呼出可能でなくてはならない。この情報は，他のインダストリー4.0コンポーネントのローカル管理およびプロセス調整のためのグローバル管理に使用される。

プロパティ（9）について：入れ子可能性

複数のインダストリー4.0コンポーネントをひとつのインダストリー4.0コンポーネントとしてまとめることができる。たとえば一台の機械がインダストリー4.0コンポーネントとなっている可能性がある。その機械自体が，たとえば機械モジュールのような複数の独立したインダストリー4.0コンポーネントにより構成されていることが考えられる。そしてそれぞれの機械モジュールもさらに細かくインダストリー4.0コンポーネントに分かれている場合がある。

6.4 標準化および規格化

6.4.1 背景

ドイツ規格化戦略によれば，規格化（英語では法律上の「スタンダード（標準）」）とは，一般に適用するため，または反復して適用するために，権威ある機関により，作業に関する規則・指針・要件などを完全なコンセンサスに基づいて策定することである。

標準化とは，ドイツ規格化戦略では，仕様の策定プロセスのことを指している。そのための文書形式はさまざまなものがあり，たとえばVDE適用規則やDIN仕様書（DIN SPEC），PAS（Publicly Available Specifications/公開仕様書），技術仕様書（TS），ITA（Industry Technical Agreement），TR（Technical Report）などがある。

昨年DKEが初版を発行し，現在ちょうど改訂作業が進行中の「DKEロードマップ・インダストリー4.0」がここでは大変参考になる。この文書の目的は，戦略的かつ技術指向のロードマップ案作成を支援することにあり，インダストリー4.0のための規格および仕様への要求条件を，経済・学術研究同盟の対策推奨事項や，連邦経済エネルギー省および連邦教育研究省の助成政策などをよく考慮した上でまとめ，行動の必要な分野を明らかにし，適宜推奨事項を提示する。また，この分野の規格や仕様書の概要も記載されている。

本プラットフォームにおいては，この規格化ロードマップが現状把握に役立つとともに，自動化技術や情報通信技術，生産技術などさまざまな技術セクターの関係者たちの間で意思疎通を図る手段としても活用されている。

6.4.2 革新の原動力としての標準化と規格化

規格および標準は，技術調達の確実な基盤を確立し，アプリケーションの相互運用性を確保し，環境や装置，消費者を統一した安全規格によって守り，将来を見据えた製品開発の基盤となり，統一した用語や概念によって関係者すべての意思疎通を助ける。

未来のプロジェクトであるインダストリー4.0を成功させるためには，標準化と規格化が非常に重要である。インダストリー4.0には，領域の境を超え，階層の区分を越え，ライフサイクルの段階を超えての，未曾有のシステム統合が必要である。コンセンサスに基づいた仕様や規格があってはじめてそれが可能となる。そのためプラットフォーム・インダストリー4.0では，研究・産業・標準化/規格化団体の間で協力を行い，抜本的な革新に必要な前提条件の整備を進めている。これには方法論による裏付けや機能性，安定性，投資の安全性，実用性，市場性などが含まれる（図29参照）。産業の現場での実践を早期に実現するためには，コンセンサスに基づく，研究の進歩に沿った標準化および規格化のプロセスが必要不可欠だからである。

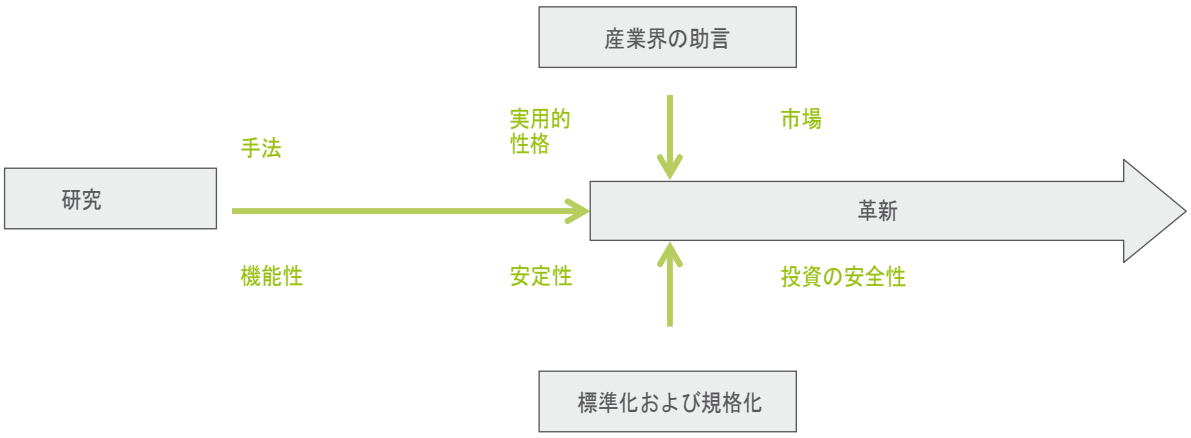


図29：標準化による革新（[10]を参考にした）

6.4.3 標準化・規格化団体の協力体制

グローバルな事業と輸出を行うドイツ産業にとっては，世界で有効な規格によって技術要件を規定することが特に重要となる。目指すのは，技術機能および利用可能性を統一する決め手となる規定事項を国際規格に段階的に盛り込んでゆくことである。ここで標的となる規格化団体は主にIECとISOである。

情報技術については，世界的に認められているIETFおよびW3Cコンソーシアム等の標準が重要な役割を果たす。インダストリー4.0のために規格化を進める目的は，アプリケーションレベルでの相互運用性向上と，ネットワークオリティの向上という二点である。

コンセンサスに基づく規格の策定には，さまざまな経路がある。図30は一般的な進め方をまとめた概要図である。出発点となるのは，特定の規格化ニーズがあることが確認されることである。規格化のニーズは，現場からのフィードバックや，新しい技術の成立，研究の成果，規制などが原因となって生じる。

国際規格（ISO3，IEC4）の成立過程をみると，三種類の一般的なルートに分類することができる。

- 該当規格化団体内で直接制定。この場合の規格制定は，該当国際機関と国内ミラー委員会が行う。その例がIEC/SC 65B/ WG 7とドイツ国内のDKE/AK 962.0.3「PLC言語」によるIEC 61131-3「プログラマブルコントローラ」の制定である。
- コンソーシアムの仕様をそのまま採用。この場合は，仕様がコンソーシアムにより策定され，その内容がほぼそのまま規格に採用される。その例としてはバッチコントロール仕様ISA S 88（ISA)のIEC 61512への採用，OPC-UA仕様のIEC 62541への採用，PROLIST仕様のIEC 61987への採用などがあげられる。
- 国内機関によるコンセンサスに基づく開発を受けて，該当規格化団体がさらに改良を加える。この場合は業界団体によって基本項目が準備され，ガイドラインないし国内仕様として公開された後に，第二段階として該当規格化団体による国際規格の制定が行われる。

これ以外の経路は図5.4.2に記載されている。電気工学分野のドイツ国内規格は現在その90パーセントがIECの国際規格に基づくものである。IEC規格はその作成段階で欧州レベル（CENELEC5）および国際レベルで並行した調整が行われた上で，ドイツ国内のDIN規格として採用される（ドレスデン協定）。ISOとCENにはウィーン協定による同様の手順がある。

ここ数年，該当規格化団体が自ら規格案や規格内容を開発し文書化するのには限界があることがわかってきた。多くの場合ボランティアとして活動している団体のメンバーには十分な時間的余裕がない。このような理由から，この代わりにコンソーシアムや業界団体が広範囲にわたって規格の準備を行う方法が多くの分野で確立されてきた。プラットフォーム・インダストリー4.0でも，その内容が該当する項目については，このやり方で進めてゆく。

その場合に規格化団体は，検証・調整・立会・助言・統合などの役割を担うことになる。関係各方面にその内容と計画を周知し，規格化プロセスがコンセンサスに基づいて進むように計らうのが規格化団体の役割である。このような役割と事務管理・編集を掌る運営者としての作業に加え，既存の規格に関する状況の分析や，戦略的に重要な分野での規格作成事業立ち上げなどでも，規格化団体は重要な役割を果たすようになっている。この意味でインダストリー4.0プラットフォームの活動開始当初から規格化団体の意義は大きかった。また，今後研究の成果を活用してゆくという段になっても，規格化団体はなくてはならないものである。

コンソーシアムと業界団体が標準化の目標とするものを比較すると，両者には根本的な違いがあるのがわかる。

コンソーシアムがひとつの規定によって完全なソリューションを記述しようとするのに対し，業界団体はガイドラインの作成やソリューションの個々の側面についての標準化を目指している。インダストリー4.0を取り巻く環境にあっては，どちらの方向性も必要である。ドイツ国内には多数の重要な業界団体がある。多くの場合，業界団体は裾野が広く，コンセンサスベースの内部組織となっているので，業界団体が公表する内容は該当業界の共同見解とみなすことができ，今後の規格化プロセスのためのみならず，産業利用をすぐにも実現するためにも確実かつ安定した基盤をなす。この点を本プラットフォームでは利用している。ここでコンセンサスに基づく進め方といえるのは，以下の条件が満たされている場合である：

- 仕様書の作成は，専門家なら誰でも参加できる審議機関が行う。いずれかの組織に加盟していることが条件とはならない。メンバーの数を限定する必要がある場合には，透明性のある，差別的でない方式によって人選を行う。
- 審議結果は早期に原案（Draft for comment）として公表する。いずれかの組織に加盟しているかどうかにかかわらず，誰でも原案を入手してコメントすることができる。
- 仕様書として公表する前に，誰でも異議を申し立てることができる異議申立手続がある。異議を認めるかどうかは，審議機関が公開の議論によって決定する。

決議された仕様書は公表され，いずれかの組織に加盟しているかどうかにかかわらず，希望者は誰でも入手できる。

すなわち，コンセンサスに基づく仕様書により，まずは国内ベースで企業内での開発プロセス用にしっかりとした標準化基盤を迅速に提供することが可能となる。そしてこの仕様書はまた，国際規格化に向けた良い出発点となる。したがって，リファレンスモデルなどのインダストリー4.0に関するコンセプトの開発をプラットフォーム・インダストリー4.0内で行い，その結果を国際規格化につなげるというのは，首尾一貫したものである。

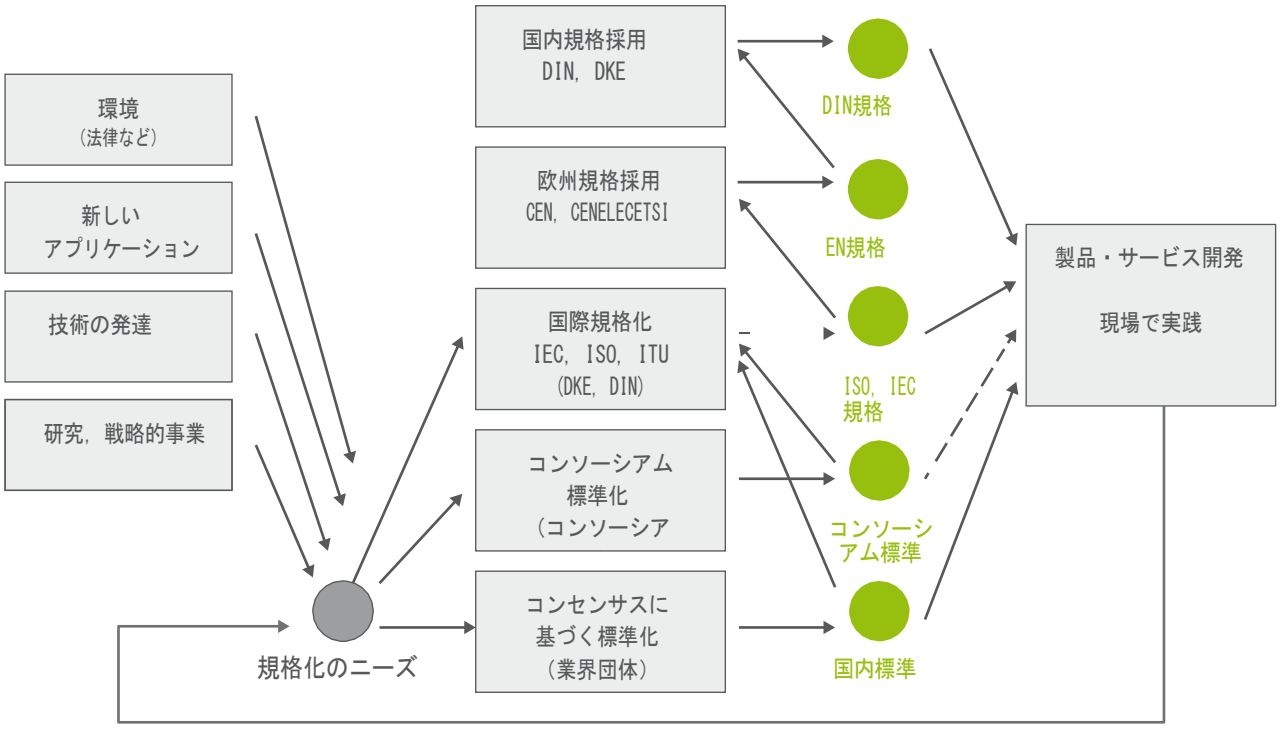


図30：規格のニーズから規格まで（[10]に同じ）

文書番号	表題	委員会
ISO/IEC 62264	Enterprise-control system integration	IEC TC65
IEC TR62794	Industrial-process measurement, control and automation - Reference model for representation of production facilities (Digital Factory)	IEC TC65
IEC 62832	Industrial-process measurement, control and automation - Reference model for representation of production facilities (Digital Factory)	IEC TC65
IEC 62541	OPC Unified Architecture	IEC TC65
IEC 61360-1 IEC 61360-2	Standard data element types with associated classification scheme for electric items	IEC SC3D
ISO 13584-42	Industrial automation systems and integration - Parts library - Part 42:Description methodology:Methodology for structuring parts families	ISO TC184
IEC 61987	Industrial-process measurement and control - Data structures and elements in process equipment catalogues	IEC TC65
IEC 62683	Low-voltage switchgear and controlgear - Product data and properties for information exchange	IEC TC17B
IEC 61804-1 IEC 61804-3	Function blocks (FB) for process control - General requirements Function blocks (FB) for process control - Part 3:Electronic Device Description Language (EDDL)	IEC TC65 IEC TC65
IEC 62453	Field device tool (FDT) interface specification	IEC TC65
IEC 62769	Devices and integration in enterprise systems; Field Device Integration	IEC TC65
IEC 62714	Automation ML	IEC TC65
ISO/IEC 2700x	Information technology - Security techniques - Information security management systems - Requirements	ISO/IEC JTC1
ISO 15926	Industrial automation systems and integration - Integration of life-cycle data for process plants including oil and gas production facilities	ISO TC184
ISO 8000	Data Quality	ISO TC184
IEC 62439	Industrial communication networks - High availability automation networks	IEC TC65
IEC 62443	Industrial communication networks - Network and system security	IEC TC65
ISO 15926	Industrial automation systems and integration - Integration of life-cycle data for process plants including oil and gas production facilities	ISO TC184
IEC 61158	Industrial communication networks - Fieldbus specifications	IEC TC65
IEC 61784	Industrial communication networks - Profiles	IEC TC65
IEC 62591 IEC 62601 EN 300328	Industrial communication networks - Wireless communication network and communication profiles - WirelessHART™ Industrial communication networks - Fieldbus specifications - WIA-PA communication network and communication profile 電磁両立性および無線スペクトル事項（ERM） - 広帯域伝送システム - 2.4 GHzのISM帯域で動作し広帯域変調技術を使用するデータ伝送装置	IEC TC 65 IEC TC65 ETSI

文書番号	表題	委員会
IEC 62591 IEC 62601	Industrial communication networks - Wireless communication network and communication profiles - WirelessHART™ Industrial communication networks - Fieldbus specifications - WIA-PA communication network and communication profile	IEC TC 6 5 IEC TC
IEC 61984	Connectors - Safety requirements and tests	IEC TC65
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related syste	IEC TC65
IEC 61511	Functional safety - Safety instrumented systems for the process industry sector	IEC TC65
IEC 62061	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems / This document and its separate amendments continue to be valid together with the consolidated version	IEC TC44
VDMA 24582	Fieldbus neutral reference architecture for Condition Monitoring in production automati	VDMA
ecl@ss V9.0	Database with product classes and product properties	ecl@ss
IEC CDD	IEC Common Data Dictionary	IEC SC3D
PROFIBUS International Profile 3.02	Profile for Process Control devices	Profibus International
Sercos	Function Specific Profiles	Sercos International
Recommendation 5th Edition 2008	XML	W3C
Recommendation 5th edition 2014	HTML5	W3C
VDI 5600	製造管理システム	VDI
…	…	…

表1：インダストリー4.0に関連があるとみなされる規格のオープンリスト

6.4.4 結論

コンセンサスに基づく規格の開発を，各該当規格化団体は世界的に長期的かつ持続的な形で行っている。ドイツ国内ではDKEとDINがこれにあたり，欧州ではETSI，CENELEC，CEN，国際規格はIECとISOである。マンデートを有するこれらの規格化団体に加え，コンセンサスに基づく標準化団体が，プラットフォーム・インダストリー4.0で組織化された業界団体と共に，仕様と規格原案の文書化を通じて規格化を推進している。ドイツ国内ではVDI/GMAがこれにあたる。各種団体の間で確立されている協力体制によって，プラットフォーム・インダストリー4.0の成果を規格化につなげるやり方はすでに馴染みのあるものである。

ただし，インダストリー4.0ではこれまでにはなかった新しい分野のテーマもあり，特にシステム指向の手法が注目を浴びるようになっている。レベル横断的かつ分野横断的なコンセプトを開発した上で，規格化も行う。これまでの作業の結果としてわかっていることは，インダストリー4.0には多数の既存規格のコンセプトを利用することができるという点である。無論，修正が必要なものもあれば，拡張が必要なものもあり，新たな規格の策定が必要となる場合もある。それでも既存の規格環境が，インダストリー3.0からインダストリー4.0への移行の道のりを今後も末長く助けてくれることになろう。関連があると思われる規格のオープンリストを表に示した。主に自動化技術の主要規格を記載したこのリストは，今後段階的にICT規格などを追加してゆき，規格化ロードマップ「インダストリー4.0」の改訂版の中で公表される予定である。

研究事項ロードマップ

インダストリー4.0リファレンスアーキテクチャモデル（RAMI4.0）およびインダストリー4.0コンポーネントの作成作業と議論によって，今後の活動に向けた第一歩となる基盤が整備された。今後研究の必要がある重要項目を以下に解説する。その際に重要な目的は，アプリケーションレベルでの相互運用性向上と，インダストリー4.0の要求に応じたネットワーククオリティの向上という二点である。

識別

識別は，モノが自動的に相互を認識できるために必要な前提条件である。これまでの議論からもすでに，商品の移動における識別，場所の識別，ネットワーク内での識別などが必要となることがわかっている。これらの分野にはさまざまな標準および規格が存在するが，その一部については新たに利用可能となった技術を追加する可能性についての議論を行う。

セマンティックス

RAMI4.0の重要なレイヤーのひとつがインフォメーションレイヤーである。このレイヤーには主にデータが格納されている。製造者横断的データ交換のためにはデータ用シンタックスを含む統一されたセマンティックスが必要となる。アイデアはすでにいくつか存在するが，その具体化のためのコンセプトを，規格化も考慮の上で作成する必要がある。「インダストリー4.0」のプロパティを包括的に定義する基盤としては，eCl@ssのプロパティ仕様などが参考になる。

クオリティオブサービス（QoS）/インダストリー4.0コンポーネントのサービスクオリティ

これはインダストリー4.0コンポーネントの重要な特性を規定するものである。設定可能かつ呼出可能となっている。コンポーネント間でサービスクオリティをネゴシエートすることも可能にする。自動化技術系アプリケーションの場合には，リアルタイム能力やフェイルセーフ性，時計同期などがそのような特性にあたる。このような特性はプロファイルに書き込むことができる。

インダストリー4.0通信

通信接続やプロトコルは，自動化技術および情報技術にはすでに多数存在する。さらに，情報通信技術による新しい方式もある。いずれにせよ，インダストリー4.0通信への要求条件に従って，各方式の適性を検証し，必要に応じて適合させなければならない。これに関しては，RAMI4.0のコミュニケーションレイヤーを利用して構造化することが考えられる。通信の例を見ると，適切な規格を特定する方法がわかりやすい。適切な規格を見つけるために，たとえば候補となる規格をすべてレイヤーに記入する。重複箇所について検討し，優先するプロトコルを定義する。欠陥がある場合にはそれを補正する。

標準機能：

さらに難しいのは，RAMI4.0のファンクショナルレイヤーにマッピングされる製造者横断的な標準機能を形成するという課題である。

情報の交換を容易にし，製造者間の相互運用性を確保するためには，統一された基本機能を規定する必要がある。したがって，シンプルで情報交換のために重要な機能をオープンな仕様で規定する必要がある。これによりユーザーが自らの機械/装置/工場のインターフェイスを適合させるコストを大幅に抑えることができる。その例としては，コンディションモニタリングの規定に関するVDMA仕様書があげられる。その中には製造者横断的な標準機能が規定されており，それぞれの製造者が独自の機能を投入（カプセル化）できるモデルもある。その場合にもデータ交換およびコンディションモニタリング機能のリンクは容易に可能である。

ネットワーキングされたシステムの安全性

7　ネットワーキングされたシステムの安全性

7.1 序論

セキュリティはインダストリー4.0価値ネットワークの「イネーブラー」である。インダストリー4.0に向けた展開において決定的に重要なのは，線形の価値連鎖が価値ネットワークに変化してゆくことである。価値創造パートナーすべてのネットワーキングがそこまで徹底的に進めば，いまだかつてなかったような形で，より多くの関係者をより深く，また時にはアドホックベースで事業プロセスおよび製造プロセスに組み込むことができるようになる。効率および生産性の向上という目標を達成するためには，機密性のある生産データやプロセスデータをパートナー同士で交換できるようにしなくてはならない。そのためにはパートナー間の信頼関係が必要であり，さもなくば重要なノウハウ（すなわち企業の核心をなす資産）を一部なりともシェアすることはできない。信頼関係を築くためには，情報やデータの交換が正当なアクセス権を持つパートナーの間でのみ安全かつ正確に検証可能な形で行われることが前提である。それを保証するのがインダストリー4.0におけるセキュリティの役割である。オフィスシステムや生産システムにおけるセキュリティが保証されない限り，機密通信プロセスに対する信頼が得られず，インダストリー4.0の実現は無理である。

セキュリティのもうひとつの課題となっているのが，安全な実装に加え，ユーザーフレンドリーな構成とすることで，顧客に受け入れてもらうことである。顧客が望んでいるのは詰まるところプラグ＆オペレート方式である。また，インダストリー4.0によって顧客対応の個別化が進めば，顧客の希望が生産プロセスに直接与える影響も増加することになる（自動車製造でロット単位が1台という場合など）。そのために必要となる緊密なB2BおよびB2Cの通信が安全かつ正確に行われ，法的安定性が担保されなければ，構想されているビジネスモデルを実現することは難しい。セキュリティ対策によって，このような要求に応えるための基盤が築かれることになろう。

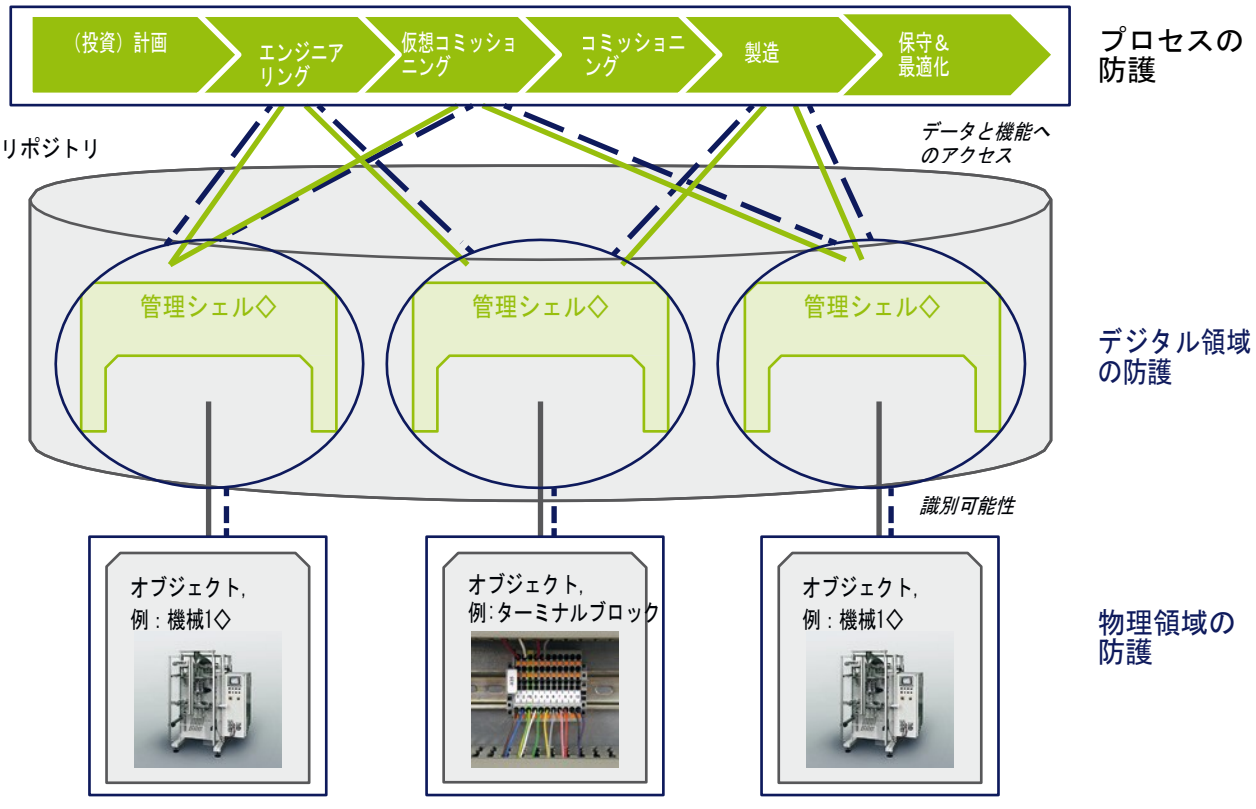


図31：安全の要求

インダストリー4.0の技術面の現状についていうなら，次のような原則が成立することになる。

物理領域およびデジタル領域，各プロセス，またこれらの領域間の通信を横断的に防護することが，インダストリー4.0成功の前提条件となる。なぜなら，分割されたセキュリティを実装しても，その迂回は容易で効果が無いからである。

安全性は他人事にあらず

企業は，企業内および企業外の多次元性を管理するという課題に直面している。インダストリー4.0では，静的で線形の組織図のような，企業内組織のいわゆる「サイロ化」はもはやあり得なくなるだろう。考えられるのは，たとえば生産プロセスがERPレベルに統合されることである（生産ネットワークが次第にエンタープライズネットワークに統合される参照）。長期的にはこのような展開が，オフィスITと生産ITの融合をもたらし，その結果必然的に静的・線形の企業組織を放棄せざるを得なくなる。それに伴って，分野横断的問題としてすべての部門に関わり，各部門に統合する必要があるような課題が増えるであろう。企業内の一貫して連続したリスク・安全管理がインダストリー4.0では必要不可欠になるだろう。多次元性が生じるのは，この管理タスクをこれまでのように「内部」と「外部」に分割することができなくなるからである。インダストリー4.0では元来内部のものであったプロセスに外部の者が直接介入する可能性が増大するため，リスク・安全管理もそれに伴う変化を反映したものとなる必要がある。これまで通り「垣根に囲まれ」，その垣根によって範囲を限定することができるような企業部門は姿を消す。価値ネットワークにあっては

企業の内部と外部の境界は曖昧となり，時間の経過と共に変化する。

このような状況では，もはや一企業が単独で自らの安全を確保することはできなくなる。考え得るあらゆる手を尽くして予防措置を行ったとしても，安全とはいえない。顧客や納入業者との連携が緊密になることで，そのインターフェイスが攻撃の的となる可能性があり，顧客や納入業者のセキュリティ管理が自らの保護レベルにも影響してくる。

最も弱い部分が価値ネットワーク全体の安全性に与える影響が今日よりはるかに大きくなる。したがって，安全性は他人事にあらずというのがインダストリー4.0の原則であると肝に銘じなくてはならない。セキュリティの確保は単独ではもはや担うことのできない共同の責任であり，それはどんな大企業でも変わりがない。

セキュリティはムービングターゲット

インダストリー4.0においてセキュリティの多次元性を考慮しなくてはならない理由には，この他にも技術の世界ですでに現在も有効なひとつの原則があり，今後インターフェイスの数が増えるにつれてさらにその重要性は高まってゆくだろう。セキュリティは「ムービングターゲット」という認識が必要なのである。「どのような事態を想定しなくてはならないのか」や「どのような対策が必要か」といった最重要事項は，ことあるごとに再吟味が必要である。なぜなら，防御戦略は必ず対抗策につながり，それがまた防御戦略に作用するからである。さらに，技術の進歩によって攻撃の方法や可能性は常に変化してゆく。技術的および人的にどのような対策を講じても，しかるべき労力や費用をかけてやはり技術的かつ人的な対策を講じれば迂回することができる。よってセキュリティについては，常に変化する動的な脅威に晒されている状態となり，常に適応していくことを要求される。いわゆる「設定したらあとはほったらかし」でも有効なセキュリティの実装などはあり得ない。これはまた，セーフティないし安全操業（＝人間を機械から守る）の原則とは根本的に異なる点のひとつである。セーフティの規定は，固定された規則であり，その一部は法律に定められたもので，統計的に評価可能な想定に基づいている。

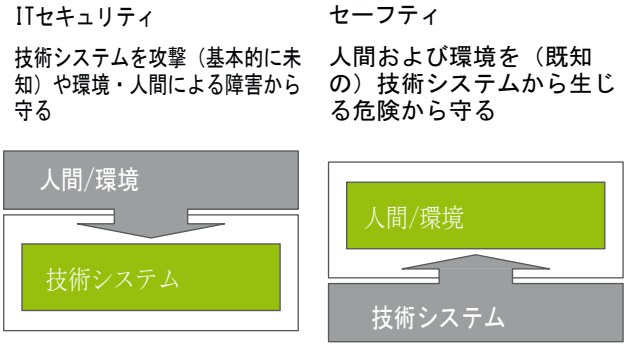


図32：セキュリティ対セーフティ

インダストリー4.0価値ネットワークにおけるセキュリティを取り巻く環境は動きが激しいため，効率的かつ適応能力のあるセキュリティリソースの活用が求められる。その基盤となるのは，企業内に存在する価値を知り，その保護の必要性を認識することである。経済効率の面を考えただけでも，セキュリティ対策は変化に対応可能であるばかりでなく，ニーズに完璧にフィットする内容でなくてはならない。必ずしもすべてのアセットを「高セキュリティ」で保護する必要はないからである。必要とされる対策を適切に組み合わせていくためには，企業の経営にあたって絶え間なくリスク管理を行ってゆくしかない。はっきりさせておかなければならないのは，何を，どれだけの労力を費やして，どの程度の安全性を目指して防御するのかという点である。その評価の結果がその後のあらゆる対策を決める手がかりとなり，ある程度の間隔で定期的な評価を行うことが望ましい。

インダストリー4.0のための100パーセントのセキュリティはない

「ムービングターゲット」の動きや技術の進歩が意味するところは，セキュリティを1）技術・人間・プロセスが一体化したものとして，また2）現場の個別事例固有のものとして認識する必要があるということである。セキュリティは，出来合いの製品のように買えるものではない。必要とされる安全対策の内容は，企業によって大きく異なる。したがってセキュリティという課題については，普遍的に有効な解決策はあり得ないというのが基本である。

7.2 想定・仮説・必要条件

インダストリー4.0の個々のアーキテクチャやモデル，装置などはまだ確定していないとはいっても，一定の技術的トレンドについての想定には信憑性がある。産業を構成する各種の要素間で自動化された企業横断的通信が増加するという想定である。セキュリティの観点においては，この想定がいくつかの結論につながる。「完結した工場」という単位での識別はできなくなる。内部と外部の責任範囲の明確な線引きがますます困難になる。これは，物理的にも，デジタル/情報技術の面でも同様である。インダストリー4.0価値ネットワークにおいて納入業者と製造者の間に緊密な通信プロセスが存在し，その中で必要に応じリアルタイム条件下で生産に関わる意思決定が行われるようになれば，場合によっては納入業者が製造業者のプロセスに直接干渉する可能性もでてくる。そうなれば相互にプロセスの障害を引き起こすことも考えられる。内部プロセスを確実にコントロールする可能性が減少し，相互依存関係が増大する。影響要因圏として決定的な，自社内の企業部門に具体的に影響を及ぼす範囲は，自らの権限の範囲を超えたものとなる。

工場の敷地が工場を囲む柵を超えて拡がるようなものである。これまでは工場の出入りを物理領域（柵＋門番/守衛）およびIT領域（イントラネットとインターネットの分離，DMZの導入）のいずれにおいても管理することができた。しかし，インダストリー4.0の到来によって，従来の区画概念は変化せざるを得ず，動的かつ必要に応じてアドホックに定義可能なものとなる必要がある。

セキュリティの仮説

このような動向と7.1項で述べた重要な認識を合わせて考えると，セキュリティに関する五つの仮説が得られる。これらの仮説は，これからのインダストリー4.0用アーキテクチャやモデルを構想するにあたって最初から念頭に置くべきものである。

1. 価値ネットワーク自体が攻撃ベクトルになり得る

   自らの企業はさまざまな手を尽くして通信および製造のレベルで保護されているかもしれない。しかし納入業者および顧客のシステムも確実に防御されていなければ，それがすべて水の泡になりかねない。インダストリー4.0環境においては，攻撃や障害が外部パートナーのシステムを通じて入ってくることを想定する必要がある。自分で管理している部門の「内部分析」だけではもはや十分とはいえない。たとえば納入業者が変わるようなケースにおいては特に，適切な予防措置やセキュリティ連携，検証などを初めから事業提携の取り決め事項に盛り込むことが望ましい。そのためには，安全対策に関する相互の（契約による）取り決めが必要となる。

2. セーフティ機能の脆弱性が増す

工業生産のあらゆるレベルでのネットワーキングの度合いが高まるのに伴って，改ざんや妨害工作の可能性がその数においてもその影響範囲においても大きくなる。機械および装置の本来の機能制御にまで不正な介入が行われる可能性も次第に現実味を帯びてきている。極端な話をすれば，改ざんすることのできない領域はもはやないということになる。

インダストリー4.0によって，機械や装置の機能制御の最も深い部分でセーフティ機能（非常停止，挟まれ防止，電磁場シールド，火傷防止など）をも含む領域にまでデジタル化が浸透すれば，該当するセーフティ機能も攻撃を受ける恐れがある。

従来セーフティ機能は分離され，場合により冗長性も担保することで，最高の可用性および信頼性を保証してきた。それがインダストリー4.0環境におけるネットワーキングによって，セーフティ装置とそれ以外の装置の間に技術的インターフェイスやいわゆる「接点」の数が増えることになる。各システムはこれにより理論上アクセスしやすくなる。これはすなわち，セキュリティの事故（外部からのハッカー攻撃など）がセーフティの事故を引き起こす（たとえば金属プレスの挟まれ事故防止システムの光バリア制御改ざんなど）可能性があることを意味する。これまで意図的に行われてきたセーフティ装置とそれ以外の装置の分離ないしカプセル化が解消される。これまで通りフェイルセーフの要請を保証してゆくことは，フレキシビリティの重要性が増す中で次第に困難になってゆく。

このような相関関係が非常に深刻な問題となるのは，人間が機械と密接に連携して働く，ロボット支援型の製造などの場面である。したがって，これまでどちらかといえば切り離して考えられてきた（現在セーフティについてのみ規格が存在する）各分野の相互依存関係についての意識を高め，安全コンセプトをそれに適応させる必要がある。

3. 検知と対応の能力が基本

さまざまなセキュリティ事故の解析結果からは，どのような安全対策でも然るべき労力を費やせば必ず迂回できることが明白である。「100パーセントのセキュリティはない」という重要な認識は，製品でも，対策でも，完璧な安全を保証できるものはないということを意味する。攻撃を検知するまでにかかる時間は現在平均で数百日間となっており，企業が検知していない攻撃の数も増加している。

さまざまな技術的および組織的対策を組み合わせたとしても，時間の余裕や調査能力，セキュリティの知識を備え持つ攻撃者（いわゆるAPT攻撃）への対応には限界がある。このように標的を定めた持続的な攻撃は，通常の安全対策では発見されないようになっている。

国家による支援を受けた組織も同じような手法をとるが，信頼関係や人物，技術などに対するそのような組織の攻撃手段ははるかに幅が広い。このような攻撃がプロによる高度なものである場合には，それを回避しようとすると過度の経済的負担を強いられることになりかねない。

通常の攻撃やサイバー犯罪のレベルにおいても，その技能水準はやはり高くなっている。事故が起きるのは時間の問題である。すべてを遮断するファイアウォールは今後も存在しない。これはすなわち，必要が生じた場合に備えて，事故を検知してそれに対応し，できる限り迅速に事態を収拾する能力がなくてはならないということを意味する。予防措置と対応措置の連動という意味での安全対策の堅牢性（検知能力も暗に含まれている）が，冒頭で述べた想定の下では，インダストリー4.0のセキュリティにとって決定的なものとなろう。今後もプロによる攻撃が迅速に，ましてやリアルタイムで検知される見込みはない。特に中小企業では，後になってから外部の者によってセキュリティ侵入や新しい攻撃方法などを知らされるケースが増えてゆく可能性がある。

しかし必要となる検知および対応の能力を強化すれば，APT攻撃の進行中ないし終了後に検知し，少なくとも後からその範囲と程度に的確な評価を行って，対応策の改善を図ることができる。そうすれば企業がより多くを検知するようになって，問題意識の向上につながると共に，効率のよい，すなわちより安価な対応も可能になる。

4. オフィス領域で知られているような検知能力を，生産領域用にも開発し提供する必要がある

現在のところオフィス通信システムの防御に焦点があてられている。これは，これまでのところ一般的な攻撃ベクトルや脆弱性がオフィスシステム（OSやブラウザ，インターネットベースの通信，データ媒体など）に関するものであるという状況のせいである。その結果として，一般的な安全対策はまさにこの領域（ウイルススキャン，Eメールおよびハードディスクの暗号化，データトラフィックとデータアクセスの管理など）に焦点をあてたものとなっている。生産領域における工業用通信用には，このような「イントルージョン・ディテクション・システム」のようなものは一般に存在しない。産業を狙ったスタックスネットのような攻撃の例を見れば，このようなプログラムが発見されるまでには数ヶ月や数年間もかかる可能性があることがわかる。

企業にとっては，ノウハウの保護という理由から，情報の把握と行動力の維持が大きな関心事である。よって，セキュリティマップ上のこのような「ブラインドスポット」を認識して計画的に解消する必要がある。これはまた，これまで考えていなかったような分野においても，組織・人・技術の面でセキュリティに投資する必要があることも意味している。

5. インダストリー4.0ではデータ分散保管がセキュリティ最大の課題となる

インダストリー4.0ではビッグデータやプレディクティブアナリティクス，知的センサ技術などを応用することで多数のサービスが新たに誕生する可能性がある。

データの専門家や解析プログラムを取り入れることで，効率性向上を可能にする（たとえば，金属プレスの打ち抜きプロセスにデータ支援型の調整方式を導入することで不良率を低下させるなど）。解析を行うには，プロセスや機械および装置などに関する非常に専門性の高いノウハウが必要になるだろう。これは，事業者が場合によっては自らのデータを外部のサービス業者および/または製造者に預けて解析してもらったり，インターフェイスを通じてサービス業者および/または製造者をデータ通信に統合することを意味する。さらに，クラウドなどのデータプラットフォームによって，場所に依存しない産業制御および生産が可能になる。

生産におけるデータの生成や転送，処理などは，場合によりデジタル化して外部のプラットフォームを通じて行われる。その結果として事業者は，技術的課題，セキュリティに関連する課題，法的な課題などに直面することになる。企業が他にも重要なインフラを使用していたり，外部の業者に委託していて，そういったものがデータに与える影響を管理するには限界がある場合が考えられる。データプラットフォームのプロバイダが自国法域外に所在している場合には，契約の規定や罰則を遂行するのが難しくなる。このようなプラットフォームは常にアクセス可能であることが技術的に要求されるのは，垂直方向および水平方向のネットワーキングを伴う価値ネットワークの要求条件であるが，これによって多数の攻撃ベクトルが考えられるようにもなる。個人情報保護および情報の安全性を包括的に保証できなければ，インダストリー4.0においてデータ分散保管を実現するのは困難である。

セキュリティ開発の原則：セキュリティは移行の形で，各企業の出発点となる状況に応じて具体化する。

ここに掲げた仮説は，文脈に依存しつつ，出発点となる既存の状況と切り離されることのない展開をみせることになろう。セキュリティコンセプトはすべて既存のシステムや装置を基盤としたものになる。セキュリティが，下位に位置づけられ，後手に回った検討事項から，「セキュリティバイデザイン」手法への根本的な変化を遂げるまでには，装置やコンポーネントなどの世代交代を経た段階的なプロセスが必要となろう。

セキュリティ標準および規格の改良についても同じことがいえる。まったく新たな標準を策定するよりも，既存の規定を修正するほうが望ましいケースが多々ある。企業の意思決定においてセキュリティ機能が純粋なコスト要因とみなされることには今後も変わりないであろう。したがって，規模の大きな企業のほうが，規模の経済性によって，該当する投資を行ったり，装置を交換したりして，新しいセキュリティレベルを実装しやすくなる。セキュリティに本格的に投資することが難しいのはやはり中小企業である。

さらに，知的センサ技術などの動向がビッグセキュリティデータとも相俟って，現在まだ孤立したプロプライエタリな領域であるために，改ざんが発見されないことの多い領域にも安全対策を導入する新たな可能性が開かれる。

7.3 インダストリー4.0 脅威の構図

今日の世界ではオフィスおよび生産領域のITに対する脅威が存在することは，もはや否定のしようがない。アプリケーションやシステムに多数の脆弱性があることが明るみにでたのはつい昨年の話である。それと同時に，企業に対するさまざまな攻撃があったことも公になった。攻撃の一例が2014年に発覚したマルウェア「Havex」である。これは産業コントロール・制御システムの情報を狙って収集するマルウェアである。その情報は製造指示書であったり，インフラ情報である可能性もあり，それをさらなる攻撃に利用することができる。別のモジュールを後からロードする可能性もあり，装置の破損につながる恐れもある。

この攻撃では，さまざまな製造者のウェブサイトが改ざんされた。そして，装置がソフトウェアアップデートのために製造者のホームページに接続すると，この通信が攻撃される。したがって顧客には，この攻撃は装置と製造者の信頼の置ける正当な通信のように見えるため，恐らく初めは何も気づかないであろう。正当なアクセスを装った攻撃が最近は増えてきており，セキュリティ事故の検知が企業にとり新たな課題となっている。検知が（もし可能であったとしても）過去を遡る形でしかできないことも少なくない。

それでも，インフラをすべて更新するよりははるかに安上がりかもしれない。検知されないまま終わる企業への攻撃の数は相当あると思われる。その被害の内容は，データの盗難から恐喝，事業・生産プロセスの損害までさまざまである。

これをみてもわかるように，すでに現在も生産装置に対する脅威は存在し，企業はそれに備える必要があることを意識しなくてはならない。インダストリー4.0は，冒頭で紹介したさまざまなトレンドを通じて，生産性の向上やプロセスおよび装置の能力向上のための新たな可能性を開く。インダストリー4.0コンポーネントの管理シェルもそのひとつである。しかし，通信が動的なものになり，サービス業者が関与することで，残念ながら攻撃の可能性も広がり，それに相応の新たな脅威が生じることになる。このような脅威に晒されているのは，管理および自動化のネットワークのどちらも同じである。

多くの場合，特に保護する価値のあるシステムはインターネットからはアクセスできないようになっており，これは生産領域にも該当することが多い。このような時に攻撃者がよく使うのが二段構えのテクニックである。まず安全対策がそれほど強力でない領域のコンピュータを一台攻撃し，マルウェアをインストールする。このコンピュータから企業のより深い部分に向けた攻撃がさらに行われる。このようなタイプの侵入は長いスパンで進行するものが多く，侵襲性も最小限であることから，検知が遅れたり，事後になってから気づくことになる。たとえばスタックスネットなどの同じように標的を定めた攻撃のことをアドバンスドパーシスタントスレット（APT）と呼ぶ。いわゆる「エアギャップ」だけではもはや十分な安全性は確保できない。

攻撃者には三通りいるとよく言われる。情報機関，サイバー犯罪者，サイバー活動家の三種類である。サイバー犯罪者は，その行為によって違法に金を稼ごうとする。そのために企業や個人を脅迫し，特定のデータを抹消したり，システムを停止させるといって脅す。サイバー活動家は，政治的動機やイデオロギーのために活動する。これは，企業の内部情報の窃盗および公開からDDoS攻撃やシステムの停止にまで及ぶことがある。この二種類の攻撃者から自らの企業を守ることが重要となる。

情報機関の攻撃者については，そのリソースがほぼ無限であることから，あらゆる攻撃経路を排除するなどとても経済的に一企業の手に負えるものではない。

このように標的を定めた攻撃のほかにも，企業が対策を講ずる必要があるのは，意図せずに引き起こされる問題で，人為的ミスや，たとえば「ドライブバイ攻撃[13]」のような無差別攻撃などがある。これは，管理ネットワークと自動化ネットワークの間でのマルウェア拡散であったり，意図しないシステムの設定ミスなどである。

攻撃ソフトウェアの開発はますます高度化しており，自動化の分野を標的とするものが増えていることが目に付く。その目的は当面のところスパイである。その例がマルウェア「BlackEnergy」である。これは特定の製造者のHMIシステムを狙ったもので，感染したシステムはその変化に気づかれないままでさらなる解析に利用される。現在のマルウェアは2008年前後からこれまでに数回修正改善が重ねられており，現在ではモジュール式に新しい機能を追加できるようになっている。このコードはあるスパイグループ[14]が書いたものとされており，つい最近も同グループがHMIシステムおよびSCADAシステム用のプログラミング用ソフトウェアの脆弱性を標的にしている。

ドイツの製鉄所にある高炉に対する攻撃が成功した事件[8]でも，その前にスパイ段階があったものと考えられ，攻撃のプロセスがこれまで不明となっていることからもその気配が濃厚である。

7.3.1 企業内に存在する価値

脅威についてさらに詳細に検討するためには，企業にとって価値のあるものとは何かを考えてみる必要がある。セキュリティという文脈においては，企業にとって最大の便益がひとつの装置にあったり，装置の一部であったり，また合金や配合のデータ，サービスなどにある可能性がある。

従来生産装置においては実質的に可用性のみに注目してきた。配合となれば機密性に焦点が移る。これは二つの例に過ぎないが，どちらも企業にとってその存続に関わる重要性を持つアセットであり，研究開発に甚大な労力が費やされてきたものと考えられる。新しいトレンドが生まれたり，新しい技術が生産に導入ないし統合されることで，サービスという形態の新しいアセットが増えることになる。たとえば（オーダー受付用や生産調整用の）ITシステムで，これまではそれほど重要な役割を果たしていなかったものや，これまでまったく存在しなかったもの，これまでは隔離された領域で稼働していたものなどが考えられる。その例としては，製品や部品のデジタルIDや機械がネゴシエートした契約の締結および管理の法的安定性確保などがある。

このようなトレンドや展開と結びついた新たな脅威について以下もう少し細かく取り上げる。

7.3.2 可用性と信頼性

事業プロセスは各種のシステムが支援している。システムとはたとえば一台の機械であったり，装置の一部であったり，またITシステムであることもある。インダストリー4.0コンポーネントの管理シェルも同じくそのひとつである。インダストリー4.0では，事業に必要な企業横断的通信システムやインターフェイスのさらなる増加と，事業プロセスがさらに動的なものとなることが予測される。

これらのシステムやインターフェイスが利用可能な状態でないと，それが多かれ少なかれ事業プロセスに影響し，よって価値創造および金銭的側面にも作用する。生産やその他のサービスの大規模な不具合は，直接の企業リスクとなる。また，たとえば物理的損害を回避するために，各種の装置を一斉に停止させる必要が生じるような危険も考えられる。

アクセシビリティが極めて高いインターフェイスでは例外なく防御が難しいのがDistributed Denial of Service（DDoS）攻撃である。この攻撃では，大量のリクエストを送って受信側の処理能力を超えるようにしたり，利用可能なネットワークの帯域幅をすべて使い切ることで，正当なリクエストが処理できなくなる。

13 予め工作したウェブサイトにユーザーを誘導し，ウェブブラウザの脆弱性を利用してユーザーのシステムを危険にさらす攻撃。

14 「サンドウォーム」

システムへのアクセスに関連したDDoS攻撃が長期にわたって持続したことで，倒産に追いやられた企業の例がすでに存在する[8]。

インダストリー4.0ではタイムクリティカルなプロセスやサービスが増えることから，DDoS攻撃の標的も増えることになる。

産業環境において極めて動的なデータを用いほぼリアルタイムで作業を行うとなると，オフィスのITセキュリティであれば通常一般的な是正措置を行う余裕はほとんどない。処理するデータには精度が要求されるのみならず，時間を同期しつつ異なるシステムから同時に取得し処理する必要がある場合もある。SCADAシステムは，異なるシステムから取得したさまざまなプロセスデータを自動的に演算し，その演算結果に基づいて制御命令を発信する。制御命令の演算に必要なデータの通信障害は，動的なインダストリー4.0環境（たとえばエネルギー業界など）においては大きな問題となる可能性がある。

7.3.3 標的としてのセーフティ

すでに述べたようなネットワーキングの進行と一企業内でのリソースの共同利用は，その程度は限られているもののセーフティコンポーネントにもあてはまることである。たとえば，他のシステムとの共同ネットワークで稼働するセーフティコンポーネントも増えている。その結果，セーフティコンポーネントも他のコンポーネントと同じようにネットワークを通じた攻撃の危険に晒されることになる。考えられるのは，安全関連機能への攻撃のほか，可用性に対する間接的攻撃である。

可用性に対する間接的攻撃

セーフティ機能に対する攻撃は，装置や機械の非常停止などにつながる恐れがある。たとえば，大量のリクエストによるコンポーネントのオーバーフローや，使用するネットワーク全体の容量超過，コンポーネントのソフトウェアのバグなどを利用して，備えられているセーフティ機能が作動しなくなるようにする。この場合セーフティコンポーネント本来の機能は維持されるため，人間や環境に危険が迫ることはないが，生産プロセスが制約を受けることになる。

安全関連機能に対する攻撃

最悪の場合には，セーフティコンポーネントの脆弱性を利用した機能の改ざんが行われ，閾値などが書き換えられてしまったりする可能性がある。結果として機能上の安全性（セーフティおよびセキュリティを含む）が保証されなくなる。人間と環境に対する損害をこのような場合に防ぐには，たとえば機械的な装置などの安全対策を追加するしかない。該当する安全機能は法律の規定（機械指令など）によって義務づけられているので，セキュリティ要件のセーフティ要件への統合作業がすでに標準化団体によって始まっている。

7.3.4 整合性

整合性は，生産に使用するデータと記録されたデータのいずれについても，極めて重要なものである。

生産に使用するデータに対する攻撃によって，製造される製品の品質を低下させることができる。極端なケースでは，たとえば製品の安全に関連する特性が変更され，それが後に人損や物損につながることも考えられる。

生産プロセスをトレースするための記録の整合性も同様に重要なもので，業種や製品によっては賠償責任の問題が生じる可能性があり，製薬業界などでは規制によって義務づけられている。

このような理由から，ほぼ例外なくどの業界でも整合性を最重視しているのだが，それが暗黙のうちに行われている場合も多く，関係者の意識では信頼性が最重要項目とみなされている。

インダストリー4.0の企業横断的価値ネットワークでは，さらに真正性[15]の問題が整合性に加わる。

インダストリー4.0においてはプロセスの調整のために高精度の同期が必要となるため，時間の整合性も重要となる。

7.3.5 機密性

すでに現在でも企業にとっては特定の情報を（多くの場合時間的な制限つきで）機密に取り扱うことが重要となっている。たとえば製法や設計データ，制御プログラムなどである。このようなデータは，その作成に多くの労力や知識が投入されていることから，企業にとって大きな価値をもつ可能性がある。

意思に反する情報の流出について「データの盗難」という表現が一般的に使われる。残念ながらこの言葉は不適切で，データは実際に盗まれているわけではなく，コピーされただけで，オリジナルのデータはまだ残っているからである。そのため「データの盗難」には気づかないことが多いというのが，実際の問題点である。

データの盗難や不正アクセスなどで主に問題となるのは，このような場合その状態を元に戻すことは不可能で，それに対応する安全対策もないことである。企業が一旦データを失ったら，その時点から不正アクセスをコントロールする術はまったくなくなる。この場合セーフティにあるようなフォールバックポジションは存在しない。したがって，既に計画の時点で然るべき対策を検討することが望ましく，企業にとって重要なデータにはその旨を表示し，その取り扱いを明確に規定することが特に重要となる。

これまでは，情報の盗難や公開を防ぐのは各企業の責任であった。インダストリー4.0では，連携する複数の企業にその責任が移ることになる。よって，データの表示や取り扱い，また責任の所在についての規定を契約に盛り込むことで，重要データの適切な取り扱いを担保する必要がある。

データの機密性を判定する際には，最終製品や機械を出荷することでそのデータがすでに自らの管理下にはなくなっていることがある点も考慮すべきである。最終製品の寸法であれば競合者が自ら測定可能であり，この場合に機密性が非常に重要なのはその製品の発表までで，その後は製品自体を見て複製することが十分可能となる。

このような機密データ処理の一例が，設計データの委託製造者への送信である。委託製造者には特定数の製品の製造を委託している。この場合には，委託製造者が希望数のみの製品製造を行い，それ以上は設計データを使用できないようにする必要がある。

もうひとつの例は，保守作業のための遠隔アクセスである。このようなケースでは，機械製造者に機械や生産ネットワークへの幅広いアクセスが与えられている場合がある。そうすると，十分な保護対策を講じない限り，稼働率や生産数などのデータをシステムから引き出したり，生産ネットワークからその他にもデータを取得することが可能となる。

機密性のある企業データとは切り離して考える必要があるのが個人情報である。ロット単位1を目指すインダストリー4.0では特に，個人情報も生産オーダーの一部として処理されることを想定する必要がある。これに関しては法律の規定を遵守した保護が必要となる。

7.3.6 改ざん（意図的および非意図的）

すでによく知られている問題に妨害工作と人為的ミスがある。これは一般に現在でも生じる問題である。企業内のネットワーキングが進み，企業横断的価値連鎖が生まれることになれば，その影響はこれまでより大きくなり，コントロールが難しくなるであろう。動的な要求条件によって（プロセス上の）責任分担と通信経路が十分に明確化されず，（技術的に）ネットワークのセグメント化ないしアクセス管理が行われなければ，まさにその通りになる。

15 「アイデンティティ盗難」の脅威を参照

アクセスポイントの数が増えれば，攻撃者による不正アクセスの危険性もさらに増大する。危険のあるアクセスポイントには，無人ステーションやオープンないし無保護のネットワークアクセス，（保守やオーダー処理用等の）他の企業との接続点などである。インダストリー4.0では，ネットワーキングがさらに動的かつ企業横断的になることによって新たな状況が生まれる。攻撃は連結された企業を起点とするものが増えると思われる。したがって攻撃の解析にあたっては，連携企業の安全管理に依存する部分が増えることになる。

主なリスクは情報の流出であるが，オーダーや生産の改ざんデータが入力されることも考えられる。その結果として機密情報への不正アクセスが行われたり，機械や装置の一部の改ざんや停止，破壊すらあり得る。

7.3.7 アイデンティティ盗難

信頼関係というものが果たす役割が，安全対策では殊に重要である。ウェブサイトを閲覧するユーザーは，送信したアドレスがまったく別の悪質な（恐らくまさにそのために予め工作された）ウェブサイトに誘導することはないと信じている。またウェブサービス側も，ログインしたユーザーが本人であることを信じている。このような信頼関係はプライベートもビジネスも同じで，通常さまざまな安全対策（機密ログイン情報やトークンキー，一意的バイオメトリックデータなど）がそれを支えている。

アイデンティティ盗難によるリスクは，攻撃者が本人を装ってその正当なアクセス権を手に入れることである。また，アクセスプロトコルにおける認証は，本物の正当なユーザーのものと変わりがない。このようなリスクを食い止めるためにさまざまな手法がある。たとえば最近では，公共アクセス可能なサービス（Gmailなど）がGeo-IPを基にユーザーの物理的な位置を判別して，複数の国からアクセスがあった場合にはユーザーに通知することが可能になっている。本物のユーザーがシステムにログインすると，セキュリティ違反があった可能性があることを知らされ，ユーザーはそれを肯定または否定できる。多くの場合，確認のために該当者とのやりとりが必要になる。そしてユーザーからのフィードバックを基に検証プロセスがさらに改善され，やがては完全に機械的に自動化されるであろう。

インダストリー4.0にとってはふたつの理由から，アイデンティティ盗難がシステムの可用性および情報の機密性に関わる深刻なリスクとなる。

関与する人間・サービス・装置・センサなどの状況は動的に変化する可能性がある。すなわちアイデンティティの数も多ければ，攻撃ベクトルの数も多くなる。さらに，機械にはフレキシブルな意思決定を行う能力がない。そのため，安全対策の検知・改善・自動化が困難となる。ここで問題となるのは，マシンツーマシンの識別というよりも，攻撃者が機械を装うという点である。このためにログイン情報や通信挙動，データ交換量などを検出・監視して，アイデンティティ盗難の可能性がある場合には検証にまわす中央監視機関が必要となることが予想される。

7.4 インダストリー4.0の安全目標とセキュリティ要求条件

水平方向および垂直方向の価値連鎖を伴うインダストリー4.0は，機械および装置のネットワーキングと企業ITとのより密接な連結，インターネットへの接続を強力に推進する。外部からの攻撃の防御と，いわゆる「内部犯行者」による改ざんの防御にあたっては，インダストリー4.0のより厳しい要求条件に対応する必要がある。

インダストリー4.0では，インダストリアルセキュリティ（生産におけるセキュリティ）とITセキュリティ（オフィス）の円滑な連携が大前提となる。このような連携の構築にあたっては，共通の標準化された安全なITインフラの実現を目指すべきである。

7.4.1 全般的安全目標

現在製造の世界で知られている安全目標は，インダストリー4.0においても同様の重要な位置づけにある。

- 可用性
- 整合性
- ノウハウの保護/機密性

これに加えて

- 真正性
- 時間の整合性，特に企業の境を超えた価値ネットワークでの
- トレーサビリティ
- 法的安定性

真正性は価値ネットワークでは必須の構成要件であり，企業の境を超えた通信が行われる場合には特に重要となる。トレーサビリティの要求は，個人と関連付けることの可能な情報が処理される場面では直ちに個人情報保護の要求から生じるものでもあり，従業員や顧客がその対象となる。いずれにせよプライバシー/個人情報保護をセキュリティメカニズムによって技術的に支援することが重要になるだろう。

これらの安全目標は，運転機能・監視機能・安全機能（セーフティなど）のいずれにも同様に適用される。システムのセーフティ（「機能的安全性」，英語では「functional safety」）というのは，機械や装置の機能により人間や環境に対する危険が生じないように適切な対策を講ずることを意味する。その際にはいかなる特殊な事例（「プロファイル」）においてもセキュリティが無干渉となるように注意が必要である。

7.4.2 インダストリー4.0用のセキュリティバイデザイン

インダストリー4.0の各種シナリオを実現するためには，情報の安全性を守るための対策を早期に検討することが必要不可欠である。ただし，技術的メカニズムを後からセキュリティに組み込むのではなく，製品開発およびプロセスにおける装置・インフラ保護のための統合的アプローチが必要となる。

目指すは，必要なセキュリティ機能を製品ないしソリューションに一体化した形で実装することである。セキュリティが該当標準に明確に規定されるというだけではなく，装置の製造者および運用者には最初からの対応が求められている。

既存のプロセスには包括的な拡充が必要となるであろう。

従来の開発プロセスは修正の必要がある。セキュリティの要求をその中に的確に組み込むためには，脅威およびリスクの分析が必要で，後の製品のアプリケーション事例を考慮することが重要となる。製品に関する安全対策の安全目標は，当事者となる製造者やインテグレーター，運用者などの保護すべきアセットや，場合により（国ごとに異なる場合が多い）当局側の規制によっても決まってくるが，たとえば重要なインフラでの使用が見込まれる場合などが後者のケースにあたる。

セキュリティデザインは（15年を超えることも少なくない）製造装置の寿命を考慮しなくてはならない。

保護すべきアセットが特定されたら，脅威およびリスクの分析を実施する。特定したリスクに即して考えられる安全対策を選択する。この時点では経済的側面も重要な役割を話す。セキュリティ対策が市場に受け入れられるのは，それが対象となるアーキテクチャのビジネスモデルに合ったものであり，それに伴う経済的負担が大きすぎない場合に限られる。

暗号化コンポーネントの選択にあたっては，輸出規制やそれに伴う手続を遵守する必要がある。これに該当するのはデータを暗号化する機能が主であり，認証や整合性のメカニズムはそれほど問題とはならない。

安全性を組み込んだ製品をさまざまな分野で使用するということになれば，実装の必要がある措置（プロファイル）の幅も広がり，さまざまな安全水準をサポートする必要がでてくるかもしれない。

安全性を考える際の焦点は現在ネットワークセキュリティの一環であるファイアウォールやVPN，ネットワークへのリモートアクセスなどにあることが多い。

これはインダストリー4.0によって変化することになろう。複雑で分散型のアプリケーションには，セキュリティバイデザインによってアプリオリに安全対策が含まれていなくてはならない。セキュリティプロファイルには「俊敏さ」が要求される。すなわち，動的な適応とネゴシエーションが可能でなくてはならない。迅速な設定（変更）がセキュリティも含め可能でなくてはならない。

従来から馴染みのある品質対策にセキュリティ独特の対策を追加する必要がある。その対策には以下のようなものがある：

- 脆弱性テスト，侵入テスト
- 生産プロセスの整合性確保，特にセキュリティプロトコルと暗号化機能
- 認証（IEC 62443準拠など）が必要になると，実現しようとする安全水準によっては，長い時間と多額の追加費用がかかる場合がでてくる。

プロセスにおいて安全機能そのものを遂行することとならんで，ソフトウェアベースのアプリケーションの確実な実装がソフトウェアの品質という意味において必要となる。着実な実現のためには，担当するソフトウェアエンジニアの教育や脆弱性に関する成果物の品質試験が必要である。品質試験の結果は解析して設計プロセスに反映させる。

7.4.3 アイデンティティ管理

インダストリー4.0価値ネットワークに参加する（機械，ユーザー，製品）ために必要かつ必須のプロパティは，一意的で偽造防止対策を施したアイデンティティであり，デジタル証明書がその証となる。デジタル証明書には，認証用のキーのほか，暗号化と復号に必要な情報が含まれている。

安全関連情報を保管するためには，信頼できる安全なメモリが必要である。セキュリティプロトコルとセキュリティ組込型アプリケーションには，必須ログイン情報をやはり安全な形で設定する必要がある。そのためには，価値ネットワークに沿ったアイデンティティインフラストラクチャ（複雑度によって単数または複数のインスタンス）が前提となり，参加ユーザーの一意的かつ整合のとれた識別とアイデンティティの関連付けを確実に行い，アイデンティティに基づいた認証および権限付与をサポートするものでなくてはならない。

必要なのは，インダストリー4.0価値ネットワークに参加するすべてのユーザーのデジタルアイデンティティ（証明書）の管理機関となる信頼できる認証局（Certification Authorities，CA）である。

効率的なアイデンティティ管理を保証するためには，セキュリティログイン情報を安全なアイデンティティによってパーソナライズ，および参加端末キーをデバイスと結びつける必要がある。

アイデンティティ管理は一貫して知的財産の保護（IP保護）に対応していなくてはならない。製品モデルや生産モデルもその対象に含まれる。ユーザーに受け入れられた適用可能なデジタル著作権管理がそのために必要な前提条件となる。

7.4.4 動的設定に対応した価値ネットワーク

効率的な価値ネットワークには，インダストリー4.0装置の動的設定/設定変更が必要となる。セキュリティ管理はインダストリー4.0装置の動的性質に対応しなければならない。そのためには，インダストリー4.0コンポーネントのセキュリティ特性（セキュリティプロファイル）を標準化された言語（セキュリティセマンティックス）によって記述する必要があり，その中には通信インターフェイス/通信プロトコルとそのセキュリティ特性の明確な記述も含まれていなくてはならない。

セキュリティ特性は，リファレンスアーキテクチャのセマンティックスの構成要素として存在する必要がある。

記述内容からは，そのインダストリー4.0コンポーネントがどのようなセキュリティ能力を有しているか，またどのような方法で必要なセキュリティ水準を価値ネットワークで達成することができるのかがわからなければならない。

コンポーネントのセキュリティ機能は基本的に各種の異なるセキュリティ水準に対応することができなければならず，それによってそれぞれの価値ネットワークについて実際に要求される条件を満たせるようになる。このよ

うな条件が揃えば，インダストリー4.0コンポーネントのセキュリティプロファイルの集約によって，結果として達成されるインダストリー4.0装置のセキュリティ水準を簡単に評価することが可能になるはずである。

セキュリティプロファイルは，動的に変化する価値ネットワークに必要なフレキシビリティにも，適切な安全機能によって対応することができなくてはならない。これは，多様なシステムが入り交じった様相を呈するインダストリー4.0では，標準化のニーズが大量に生じることにつながるだろう（KITSロードマップ – ITセキュリティ規格化ロードマップ，DIN/DKE，2015/02/17参照）。

いずれにせよ従来の考え方（通信およびネットワークを中心としたセキュリティ）はアプリケーションレベル用の複雑なセキュリティアーキテクチャへとシフトすることになるだろう。

7.4.5 仮想インスタンス用のセキュリティ

インダストリー4.0では生産の「仮想インスタンス」が重要な役割を果たす。安全の要求を物理世界で実現するのと同時に，このようなバーチャルイメージのセキュリティも同様に必要となる。

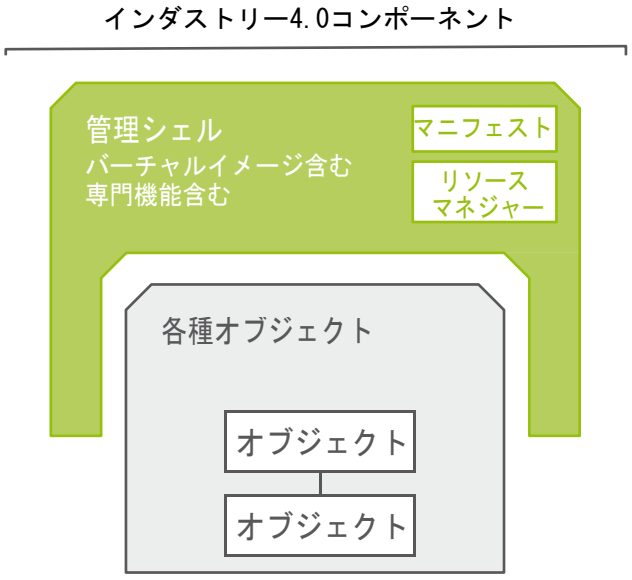


図33：インダストリー4.0コンポーネント

論理ビューにおいて，インダストリー4.0コンポーネントには単数ないし複数のオブジェクトとひとつの管理シェルが含まれ，この管理シェルにバーチャルイメージおよび専門機能のデータが入っている。

要求条件：

上位システムの種類によっては，管理オブジェクトを複数の上位ITシステムに配置する可能性が必要となる。

「仮想インスタンス」の配置（オフィスプラットフォームまたはクラウド）によって，セキュリティ環境条件が物理世界とは異なってくる。勿論物理レベルとのインタラクションも，安全かつトレーサブルに構成されていなくてはならない。よってアプリケーションレベル用の複雑なセキュリティアーキテクチャが必要となる。ノウハウの保護と整合性がここで特に重要な要求条件となる。従来のセキュリティの境界線をそのまま「仮想モデル」にマッピングすることはできなくなるだろう。エンドツーエンドセキュリティが重要な項目となる。セキュリティアーキテクチャの具体化に大きく貢献する可能性があるのは，リカバリー機能の一環としての「仮想インスタンス」である。その中にはセキュリティ事故発生後に物理環境を回復するために必要な情報がすべて含まれているはずだからである。

7.4.6 予防と対応

予防と対応はいずれも必要：それ以上何もする必要がないような出来上がったインダストリー4.0のセキュリティソリューションはない。

攻撃者のノウハウと装備は常に向上し続けている。よって攻撃ベクトルも常に変化してきており，実効性のある対抗策の効果的拡充が求められている。

予防的な安全対策に加え，レスポンスのメカニズムも絶対に必要である（モニタリングとイベントハンドリング，インシデント管理）。ルールベースの解析を伴うセキュリティメッセージ用のセマンティックスを標準化すれば，積極的レスポンス管理の必要条件を整備することができる。1年365日24時間体制のセキュリティオペレーションセンター（SOC）にすべての活動をまとめることで，セキュリティのあらゆる側面について的確な情報収集と分析評価を行うための業務体制が整備される。

セキュリティは「一回限りの問題」ではない：セキュリティを一回限りの行動で達成することはできない。攻撃者が利用することのできる新しい技術の登場や普及している製品およびコンポーネントの脆弱性の発見と公表によって脅威の状況は刻々と変化している。製造者や運用者はパッチやアップデートによってそれに対応する態勢を整える必要があり，新しいバージョンのセキュリティを導入する可能性を見極めて，プロセスの計画に盛り込んでゆかなければならない。セキュリティのコストが嵩むのは製造者側と運用者側のいずれも同じで，あらゆる関連プロセスでオーバーエンジニアリングを徹底的に防止する必要がある。

検討の目的は常に横断的セキュリティアーキテクチャの実現である。その中ではアプリケーション環境のアーキテクチャ全体と，標準化・開発・生産・管理などのあらゆるプロセスを考慮する必要がある。

セキュリティがその本筋においてプロセスの問題であることには今後も変わりなく，セキュリティチップ1個だけでセキュリティを保証することはできない。

それぞれの生産環境独特の環境条件を考慮したIT構造の適応を行うことが望ましい。

7.4.7 アウェアネス，職業訓練，社員教育

組織的な措置が重要な役割を果たす。セキュリティ対策とその必要性に関する関係スタッフの意識強化を図るためのアウェアネス教育を，関与する各組織（製造者，装置製造者，運用者）で実施する必要がある。これによりセキュリティ対策に対する理解を得やすくなり，対策実施の質が向上する。

セキュリティの管理や機能，プロセス（キー管理，監査機能，イベントハンドリング）のためのインフラと，適切な訓練を受けた人材の確保が必要となる。製品およびソリューションの製造者側から提供されるユーザーガイドラインもプロセスに組み込む必要がある。パスワードやデータ，データ媒体等の取り扱いや，定期的なデータ保存などがこれに含まれる。

7.4.8 作業性

インダストリアルセキュリティ機能は，大量の予備知識がなくても操作できるものでなければならない。特に保守等のサービス時の不具合解消などに関してこの点が重要となる。プラグ&オペレートがセキュリティソリューションには特に好ましい。

7.4.9 標準および規定

そのためインダストリアルセキュリティは，まさにインダストリー4.0との兼ね合いもあって，現在業界団体や規格化団体での議論の対象となっている。

国際規格IEC 62443「産業用通信ネットワーク — ネットワーク及びシステムセキュリティ」は，四種類のセキュリティレベルに基づいたインダストリアルセキュリティ評価基準の枠組となる。産業用自動化システムのセキュリティに関する七つの基本要件（Foundational Requirements，FR）があり，それがさらにシステム要件（System Requirements，SR）と強化策（Requirement Enhancements，RE）に細分化されている。セキュリティレベルは，それぞれ1セットのSRとREに基づいている。

各コンポーネントのセキュリティ能力は，要求されているセキュリティレベルに応じてシステム統合時に考慮する必要がある。それと同時にプロセスも要求されているセキュリティレベルが達成できるように構成する必要がある。

IEC 62443は将来認証に使用される見込みである。

VDIガイドライン2182に記載されている産業自動化のITセキュリティに関する手順モデルは，コンポーネント製造者および機械製造者と運用者の活動が噛み合わさったものとなっている。運営者はリスク分析の一環として潜在的な脆弱性を特定し評価する。製造者は，セキュリティコンセプトやセキュリティソリューションの作成に必要な情報（関連するネットワークプロパティなど）をインテグレーター/機械製造者ないし運用者に標準仕様の枠内で提供しなくてはならない。このガイドラインがIEC 62443に取り入れられている。

セキュリティプロセスを確立し実現する組織の能力を適切な基準によって判定する必要がある。

動的設定を理想とするインダストリー4.0価値ネットワークの考え方は，変更を加えると認証/営業認可の喪失につながる現行の規制や規格の規定とは真っ向から対立するものである。したがって動的性質にも対応した規則が必要になる。干渉のないセキュリティメカニズムによる独自のセキュリティをすべての参加端末に徹底することがその前提となる。

7.5 模範的なセキュリティ対策

本項で紹介する模範対策は，ジェネリックなツールボックスのようなものと考えて頂きたい。ITや各種の専門部署ないしセキュリティコンピテンスセンターなどの本部組織が企業のITセキュリティ改善のために効果的な対策を開発し実現するにはどのような方向性が考えられるか，その代表的なアプローチを紹介する。その中でも特に，現時点でもすでに将来重要となることがほぼ間違いないとみなされているものの，その普及や具体化が今はまだ進んでいないアプローチを取り上げる。したがってこれは，インダストリー4.0のためにこれからやり遂げなければならない産業用セキュリティの転換を巡る議論を抜粋したものとなっているが，対策目録として完成しているわけではない。コンセプトレベルから量産レベルに発展させるには，なによりも要求条件をもっとはるかに詳細に規定する必要がある。

7.5.1 セキュリティアーキテクチャ

アーキテクチャレベルでは，インダストリー4.0用セキュリティの設計にあたって検討すべき対策がいくつかある（セキュリティバイデザイン）。

職務分掌（segregation of duties/separation of duties）が現在生産において行われるのは，ほとんどの場合管理者権限とユーザー権限の間のみであるのが一般的である。通常コンポーネントは，完全な権限を有する管理者アクセス（スーパーユーザー）によって稼働し，生産領域を超える権限を持っている場合も少なくない。これまで生産においては合理的な理由から可用性およびデータの整合性という安全目標に焦点が絞られており，機密性や真正性はそれほど重視されていないという事実がその原因となっている。

これはインダストリー4.0に伴って変化する（変化せざるを得ない）であろう。なぜなら，インターネットと接続された保護されていないコンポーネントに対するサイバー攻撃が成功する確率は非常に高いからである。その上コンポーネントが自らの領域を超える管理者権限で稼働しているとなれば，その影響はことさら大きいものとなる。機密性および真正性という安全目標がなおざりにされていると，それがいずれは（たとえばインターネットを通じたサイバー攻撃などによって）可用性やデータの整合性にも影響を及ぼす恐れがある。この例からわかるように，システム設計，すなわちモジュールや機械，生産装置から価値ネットワークまでを複数の分離された領域に分割することは，アーキテクチャに必要な措置である。この分割は論理上のものもあれば，物理的なものあり，データアセットが保存された形で存在するか，転送された形で存在するかというものや，アクセスが分離されたドメインということもある。後者の場合にはドメインの境界で認証が必要になる。また，分割は垂直方向のもの（同じモジュールの管理者ログイン対操作員ログイン）や水平方向（異なるモジュールで分離された管理者アカウントと操作員アカウント）のものがある。ここでいう措置とは，分析に基づいて，設計の適正な位置に隔離用の境界線を挿入するということであり，セーフティに関連する部分など，既知の重要項目の区分との兼ね合いも重要である。（恐らく現実的ではないと思われるが）もし分割を最大限行ったとしたら，ひとつひとつの機能がそれぞれ独自のセキュリティドメインとなり，固有のアクセス管理，権限などのセキュリティ機能を備えることになろう。

これと深く結びついており，セキュリティの議論で頻繁かつ繰り返し取り上げられるのが，ネットワークのセグメント化である。しかし，「内部」と「外部」，または信頼性の異なるネットワーク領域，安全の必要性に差があるゾーンなどの明確な区分は，インダストリー4.0においては，次第に（サブ）ブロックレベルのより粒の細かい区分に取って代わられることになろう。ファイアウォールはインターネットとの通信を必要とするシステムの数が多いために穴だらけ同然になるか，あまりに複雑になりすぎて，無数にあるルールを誰も掌握できなくなり，いくつかのルールが相互に矛盾する恐れが生じる。

ルールが適正でもその数があまりに増えすぎて，進行中の通信に後れを取ることなく検証をするのが次第に困難になってゆく。この傾向はインダストリー4.0によってさらに強まることになる。自動化が進むことによってプロセスの時間的密度が高まるからである。その結果として，ファイアウォールや構造上のセキュリティ対策といった形の従来の周辺保護は次第に効果が薄れてゆき，それと共に重要性も失われてゆく。したがって重要なのは，将来インダストリー4.0と共に変化してゆくことになる各種の条件を，個々のコンポーネントやワークフローを設計する時点ですでに考慮に入れておくことである。措置として重要になってくるのは，通信レベルでの分離をこれまでにより大幅に小粒の構成としつつ，ルールがかなり静的なファイアウォールによる形式的に動作する一般的な分離から，以下の要素を組み合わせたシステムに移行することである。寛容なルールによるファイアウォール。このルールにネゴシエートの余地はなく，通信用のガードレールとなる。インダストリー4.0の生産では決して許されない事項はすべて禁止される。たとえば，外部の上位コントローラからの内部にある分散型アクチュエータを制御するアクセスなどが考えられる。これを補足するもうひとつの措置として，生産ユニットの各種モードを区別する。モードにより通信ルールが許可されたり，禁止されたりする。その例としては，一般的な遠隔保守のケースがあげられる。遠隔保守作業中は，他の生産ユニットとの通信が禁止される。このようなタイプの通信制御改良方法は別の次元にも拡張することが可能だが，その詳細は将来の生産通信ネットワークに対する要求条件によって変わってくる。

「ディフェンスインデプス」もアーキテクチャの措置であるが，製造所を孤島として認識し，敵の侵入やアクセスから守ろうとする慣習から脱却する一方で，個々の対抗策で必要な安全水準を達成できるという仮説に別れを告げるものである。その代わりに，ひとつひとつの部品，つまるところあらゆるデータアセットを，それぞれ独立した保護すべきコンポーネントとみなし，たとえば認証や暗号化などによって守ろうとする。

また同時に，さまざまな攻撃者がいて，攻撃能力にも差があることを考慮し，ディフェンスインデプスによって最善のケースではどのタイプの攻撃者も最も早い時点でそのタイプに合わせた対策に阻まれて挫折すると考える。すなわち，さまざまなレベルの適切な対抗策を組み合わせて用いることで，コストパフォーマンス良く適切な保護を構成する。その中には，インフラストラクチャのほか，通信経路，データ通信に用いられるプロトコルが含まれる。「ディフェンスインデプス」は，コンポーネント内で処理され（一時）保存されるデータの暗号化に始まり，認証およびデータアクセス権限付与用の特殊なデータ通信プロトコルからエンドツーエンド暗号化にまで及ぶ可能性がある。その際にアクセスが人間によるものか機械によるものであるかは問題とはならない。どのような対策の組合せが総合的に最善の安全をもたらすかは，個別の分析によって，統一的な総合戦略にも沿った形で判定する必要がある。

ルールを厳密に遵守しつつ，フレキシビリティを維持することが，アーキテクチャパラダイムとして必要になるものと思われる。つまり，ネゴシエートすることができない「ガードレール」が存在し，生産においてセキュリティポリシーとして厳密に実行しなくてはならない。その例としては，個人（操作員）と関連付けられる情報の全域にわたる暗号化があげられるが，これは個人情報保護の理由から，企業の規模や地域などにかかわらず，最低限の対策として常に必要になるだろう。しかし，このガードレールで囲まれたグラウンドの中では高いフレキシビリティ（上記安全目標「動的設定に対応した価値ネットワーク」参照）がさまざまな基準について要求される。上の例でいえば，これはたとえば地域によって異なる（法律の）規定を反映させることを意味し，どのような個人に関連するデータを収集・保存・（どこに）送信・（いつまで）保管することが許されているかを反映させる。また，対策の安全水準（たとえば単純なパスワードに比べた場合のマルチファクター認証による攻撃に対する抵抗力の増加，ただし実装クオリティの向上による場合もある）およびセキュリティ対策への時間的要求条件，またそれ以外にも多数存在するセキュリティのさまざまな特徴などには広い範囲でアプリケーション事例ごとにばらつきがでることが予想される。

それに加えて，自律性や遅い時点での（趣旨に適ったオーダーの）変更などによって，予測不可能なイベントや通信の変動が生じるであろう。このような類の動的性質は現在の生産環境では一般的ではなく，特にセキュリティ対策が新たな課題に直面することになる。フレキシブルなセキュリティを安全かつ確実に実現するための方法としては，本来の生産通信から独立したセキュリティ管理ネットワークが考えられ，このネットワークを通じてセキュリティに関係するランタイムの設定変更を行う。このような手法の商業的評価を行うには，費用と評価の対象となるリスクを比較できるようなリスク分析が必要となる。

また，ルールの厳密な実行を，ソフトウェアアルゴリズムにおける（設定変更可能な）ルールによる動的設定ではなく，静的設定ないしハードウェアによって実装することも可能である。

7.5.2 アイデンティティ管理

どのユーザーがいつどの機械にアクセスしているか，またアクセスすることが許されるのかがわかっていてはじめて，不正アクセスを効果的に検知して阻止できる。これがアイデンティティ管理につながる。

人間と技術的エンティティ用の電子アイデンティティの全域にわたる導入と，それに基づく認証および権限付与方式によって，上で要求されているような職務の分掌およびそのアクセスならびに強制アクセス制御と最小権限の原則が実装される。すなわち，アクセスには必ず認証と権限付与が必要で，アプリケーション事例で必要な最小限の権限のみが付与される。

インダストリー4.0の自動化および自律化が進行するのに伴い，上述の措置はシステムや機械，装置についても導入する必要が生じることになるが，他のコンポーネントを制御する作用があるものについてはことさらである。

このように一貫したアクセス認証の前提条件となるのは，該当プロセスにおいてリソースのアクセス権を有する人間および機械のすべてのアイデンティティのリストが生産ネットワーク全体について存在することと，必要な作業内容を反映した各種のロールおよび権限のモデリングである。

さらに，現在有効なアクセスルールを規定するポリシーがシステム全体で利用可能であり，整合性がとれている必要がある。これは，国際的に事業を展開する大企業にとってはまさに困難な課題である。プロセスやロール，権限，アイデンティティなどの数があまりに膨大で，一箇所に保管して管理することができないからである。世界中に分散した事業所とこのリストへのアクセスを考えると，集中型のソリューションは不可能と思われる。企業全体で一意的なアイデンティティを付与できるようにするには，企業内で使用されているすべてのアイデンティティにアクセスすることができる検証メカニズムが必要で，新たに作成しようとするアイデンティティがすでに企業内に存在しないかどうかを確認してから，新しい一意的な識別子を付与できるようになっていなくてはならない。ただし十分に考えられるのは，アイデンティティを管理する複数の分散型データバンクが存在するという可能性である。このような分散型のケースでは，新しいアイデンティティの付与や既存アイデンティティの管理にあたって，該当するアイデンティティがすでに存在するかどうか，またどこでそのアイデンティティを管理しなければいけないのかについて，存在するすべてのデータバンクとの対照によって確認することが可能であることを保証しなければならない。分散型の構成は，ロードバランシングとフェイルオーバーメカニズムが組み込まれた高可用性アーキテクチャが前提となり，これによりすべての使用されているデータバンクが常に利用可能であることが保証される。ただし保守作業のための時間枠にも配慮が必要で，さもなくば自社内のアイデンティティへのアクセスが保証できず，たとえば従業員証や証明書などの発行・検査・回収などができなくなる。以上のような課題があるのは，上述のその他のデータについても同様で，たとえば必要なロールや権限が地域によって異なる構造であっても，中央で監視・記録できるような方式を導入する必要がある。システムおよびその構成要素のアイデンティティの数のほうが，人間のアイデンティティよりもはるかに多くなることが予測される。

たとえば，従業員証は企業内のひとりの人物のアイデンティティを記したものであり，従業員証のつくりによって，部屋や建物への出入りをコントロールしたり，ソフトウェアへのアクセスを制御することができる。

従業員証の作成時には人物の身元を公文書（身分証明書，旅券等）によって認証し，従業員証番号を企業全体で一意的に付与されたその人物のアイデンティティと結びつける。これとは別の権限付与プロセスを通じて出入りおよびアクセスの権限を付与することができ，従業員証のつくりによってはそのICチップに該当する権限の証明書を格納できるようになっている。証明書には原則的に有効期限があるが，これには定期的な検査（再認証）を強制するといった意味合いがある。アイデンティティと結びつけられている権限に従って，どのアイデンティティからでも一度付与された権限を削除することができる。会社を退社した場合などがその例である。また，従業員証を紛失した時には，その従業員証から権限を削除したり，従業員証を完全に無効にすることもできる。これはどの企業でも，従業員証の発行・検査・回収に使用されている集中型のプラットフォームを通じて行うことが望ましい。

システム設計において権限を分離して複数のユーザーに分割し，各ユーザーはその作業に関連する権限だけを有する（最小権限，職務分掌）ようにすることで，外部の攻撃者にとっては（暗号化された）情報にアクセスするのがさらに難しくなる。

7.5.3 暗号 – 機密性の保護

機密扱いの情報がデータ媒体に電子的に保存されていれば，まず間違いなくその情報を不当に入手しようとする者がいるものと考えなくてはならない。しかし，第三者による不正アクセスがあったとしても，一貫して十分な強度がある暗号化を行っていれば，その情報の解析を極めて困難にすることができる。暗号化アルゴリズムが良ければ情報の機密性の保護が向上し，（鍵無しでの）不当な復号にかかる労力が極端に大きくなる。データ通信は何箇所かを経由することが多い。転送はそれぞれ暗号化されていても，一時保存が平文で行われていれば，第三者によるデータの盗難やデータの改ざんの危険がある。

エンドツーエンド暗号化はデータの改ざんを難しくし，不正アクセスやデータの盗難があった場合にデータの解析を困難にする（「secure-the-weakest-link」）ものの，不正アクセスやデータの盗難を防ぐことはできない。たとえば非対称暗号では，送信者が受信者の公開鍵を使ってデータを暗号化し，さらに暗号化して送信し，暗号化して保存する。非対称暗号や対称暗号をどのように使うかは，アプリケーション固有の条件を考慮に入れたコンセプトによって決まる。この例としては生産機械で使用する交換可能な製造者の製法データがあげられる。このケースでは，製造者から運用者へ，そしてさらに機械への送信の暗号化を規定することで，インダストリー4.0ではより大きな価値をもたらすようになる有償の配合データが運用者に開示されてしまうことを阻止する。運用者は通常機械の管理者権限を持っているので，機械への製法データの保存も暗号化した設計とするべきである（または，製造者のみが自らの署名入りのコードでのみ読み取り可能なメモリ領域を使用する）。製法に基づくプログラムのプロセスについても暗号化するかどうかは，運用者や外部の攻撃者によりランタイム分析が行われるリスクを評価して，それを阻止するために必要となる多大な労力を正当化するだけの危険であるかどうかを判断する。対称暗号を使用する場合には，ローカルの秘密鍵用に十分安全なメモリと適切なインフラが必要で，特殊なハードウェアセキュリティエレメントが必要になることも多い。それに加えて，もしくはその代替策として，機械ごとに個別の鍵を使用することで，攻撃の被害を限定することもできる。この場合には，さらに製法データの使用を特定の機械に限定することも可能となり，ライセンス管理にも利用できる。

7.5.4 暗号 – 整合性の保護

暗号は，適切な形態のチェックサムを署名と組み合わせて使用することで，整合性の保護にもすこぶる適している。

インダストリー4.0における措置としては，整合性および真正性の保護に有効である。その例としては，組み込みシステムの基本システムソフトウェア（組み込みOS）の保護をあげておく。組み込みシステムは，安全な起動プロセスを必ず用いた設計を全域で徹底することが望ましい。これは，フィールドでは変更することができない（読み取り専用メモリ，TPMなど）ソフトウェアの最初の部分がまず，その次の領域にあるソフトウェアコードの整合性をハッシュおよび署名を用いて検証してから起動するシステムである。これは必要に応じて複数の段階で行うことも可能であり，稼働時に信頼できるコード基盤となる。ハードウェアセキュリティモジュールは攻撃に対するリジリアンスを高めるために有意義である。インダストリー4.0に関しては，どうすればこの措置を全域で実現できるかを確認する必要がある。特にその費用が相対的に高くつく場面で問題となる（シンプルなセンサの場合など）。

上述した製法データの例では，演算時間に対する要求条件がそれほど厳しくない場合（一般的な対称暗号方式は同等の強度の非対称方式と比べて演算が速い）および安全な保存場所の適切なものがローカルになく（対称方式で必要となる秘密鍵用），製法データの真正性のほうが機密性よりも優先される場合には，非対称暗号を使用することができる。真正性の検証には製造者の公開鍵があればよく，公開のものであるので保存に安全なメモリ領域を必要としない。

どの暗号方式や暗号化アルゴリズムを具体的な事例で使用するかは，必要な保護期間，利用可能なリソース（演算能力），鍵保存用のローカル秘密メモリの存在および導入の可能性対集中型インフラ（公開鍵インフラ），オンライン接続の可用性（集中型管理，リボケーション），明るみに出た攻撃などのさまざまな基準によって決まる。

暗号によって安全のタスクは全体として容易になるが，鍵の取り扱いには注意が必要である。鍵を紛失した場合にはデータを損失する恐れがあり，鍵が悪者の手に渡れば，知らぬ間に暗号化されたデータにアクセスされてしまうことも考えられる。しかしそれでも，暗号なしで全域にわたる保護を実現するよりも，鍵を数少ないところに集めて守る方が簡単である。

確立された方式であるPKIなどがそのために利用できる。専用のハードウェアコンポーネント（数多くのセキュリティ機能とさまざまな攻撃方法に対する強力な防護を備えたセキュリティチップ）も利用可能である。アプリケーションとリスクの状況に適応したコンセプトがあってはじめて暗号がその威力を最大限発揮する。

7.5.5 安全な遠隔アクセスと頻繁な更新

製造者がインターネットを通じて工場の機械やロボットの遠隔保守を行うのが一般的なやり方である。その際には製造者の技術者がインターネットを通じて企業内にある保守対象の機械に直接アクセスし，ファームウェアアップデートを実行したり，性能改善のために設定を行ったりする。異なる企業の（共同のプラットフォームによることもある）連携には，各種のユーザーの認証を正しく行うという大きな課題が秘められている。なぜなら，自社の従業員は人事システムを通じて一意的に識別できるのが普通だが，提携先や顧客，製造者の従業員は識別できないからである。各企業にはそれぞれ独自のアイデンティティ管理があっても，提携企業間には技術レベルで確立された信頼関係がないというのが一般的である。

このような信頼関係は「フェデレーテッドアイデンティティ管理（FIM）」と呼ばれる方法で構築することができる。この方法では，すべての連携企業が信頼する（必要がある）外部のアイデンティティブローカーが，リクエストをしているアイデンティティ（それが人間であるか機械であるかに関係なく）が本物であるかどうかを検証する。この検証は，次のファクターのうち二種類以上を組み合わせて使用するマルチファクター認証によって行うことができる：占有（ドングル，スマートカード，トークン），知識（パスワード，キーフレーズ），バイオメトリックス（指紋，虹彩スキャン）。そして認証が行われたら第二のステップとして，このアイデンティティにはアクセス権限が付与されているか，付与されている場合にはどのような権限か，そして希望のシステムへのアクセスが許されるかどうかを企業内で検証することができる。少なくともこの時点では横断的な標準が必要不可欠である。

使用されているコンピュータシステムについても同じく信頼の問題が生じる。マルウェアやウイルス，ましてやバックドアなどの危険が，運用者が管理していない遠隔保守に使用される製造者のシステムから生じないことを確実にするために，（事実上）標準化されている仮想化技術を用いることができる。その際に運用者と製造者は使用を許可するイメージを共同で規定し検査すればよい。稼働時に製造者にとって重要なのは主にVMインターフェイスとVMプロセス環境における必要な保守ツールの可用性であるのに対して，運用者の関心は第一に生産のリスクを回避することにあるからである。生産システムの観察・手入れ・分析のための連続的サービスに向かってインダストリー4.0が進化するのに伴って，この措置は継続的に改善してゆく必要がある。その例としては，生産からの操業データ流出の管理をあげておく。

頻繁な更新ないし必要に応じてソフトウェアのバグを修正する可能性は，ソフトウェアの比重が増してゆくネットワーキングされたシステムに対する要求であり，生産環境においては安全操業などに関する認証の内容に矛盾するものとなる。
考えられる対応策としては，認証されたシステムをセキュリティゲートウェイによってネットワークに対してカプセル化する方法がある。セキュリティゲートウェイの機能は非常に大きく異なる可能性もあるが，その核心においてはカプセル化されたシステムの可視化とそれに伴う攻撃の標的となる可能性に対処するためのものである。モジュール化がますます進むことを考えれば，これはゲートウェイの小型化と同時に，産業関連プロトコルおよび保護メカニズムのサポートの幅を広げることを意味する。プロトコルやISO/OSIレイヤーの数が増え続ける中でのリアルタイム通信監視を行いつつ，誤検出をも防止する可能性の限界を押し上げて行かざるを得ないだろう。これと組み合わせて実施すべきもうひとつの措置として，認証後でもフィールドでの更新を許す方式の導入が求められており，そうすればたとえば適切なモジュール化などとも合わせて，可視化され，そのために攻撃の標的となる恐れがある部分だけでも認証の核心部分から切り離して更新可能とすることができるかもしれない。

認証メカニズムは，保護されたデータにアクセスできるのは権限を有するユーザーアイデンティティのみであることを保証する。しかし従来のパスワードや占有を用いるシングルファクター認証では，ユーザーアイデンティティに権限が付与されているかどうかの検証だけで，正しいユーザーがそのユーザーアイデンティティを使っているかどうかは検証しない。

受信者の秘密鍵が流出していないことが確実ならば，メッセージを復号して読むことができるのは宛先の受信者のみである。鍵を破ることはまったく不可能ではないが，比較的大きな労力を必要とし，現在の技術では個別に標的を定めた形でのみ可能で，全域にわたる一斉の鍵破りなどは不可能である。

一貫した暗号化を行うには，送信者および受信者がそれぞれ有効な認証局の鍵を持っており，それを使用することと，暗号化した通信および暗号化したデータ保存が使用されているインフラで技術的に可能であることが前提となる。それには適切なプロトコルやハードウェアおよびソフトウェアを使用することで，暗号化によって増加する演算量とパフォーマンスの低下を我慢できる程度の最小限に抑えることも重要である。

これは，企業内のプロセスのみならず，製造された製品内部のプロセスおよびデータフローについてもいえることである。

7.5.6 プロセスと組織的措置

企業内ではデータセキュリティリスクの管理を，リスク管理システムおよびインシデント管理システムを含む適切かつ包括的なセキュリティ管理が支援するというのが理想的なケースである。リスク管理の役割は，既存のリスクの特定と対応であり，それによりリスクを可視化して，各専門部署と協力し，コンプライアンスに配慮した上での，これらのリスクへの対処方法を組織的に定義できるようにする。特定されたITセキュリティのリスクに対応する方法は基本的に四種類ある。受容，低減，解消，転嫁の四通りである。

ITセキュリティリスクに適切に対応するためには，そのリスクを認識している必要がある。認識しているリスクでなければ，効果的に取り組むことができない。企業内の関連する部署や部門がみずからの所轄を勝手に定義したために，取りこぼし事項がでたり，横断的事項の押し付け合いになったりする危険が生じるのを防ぐためには，組織内に横断的な職務を設け，企業全体で有効な職務と役割の分担を明確に定義することが重要である。まだ存在しない場合には，この業務に専念するポスト（「チーフインフォメーションセキュリティオフィサー」，「プロダクションインフォメーションセキュリティオフィサー」）を創設することが望ましく，緊密な調整と協力を通じて，ITセキュリティを全企業をあげての総合的なプロセスとしてとらえるのがその使命である。

通常そのようなまとめ役が最初にやることは，包括的なモニタリングコンセプトを策定し具体化することである。そのために既存のモニタリング措置を継続ないし集約してもよい。しかし，ドキュメンテーションや主に管理者が対象となる安全関連中央システム（鍵の集中保管）へのアクセス記録解析など，これまで注目されることの少なかったセキュリティ関連部門の多くは，少なくとも生産の分野では一般的なものではないため，新たに設置する必要がある。

さらにインダストリー4.0では，企業および国の境界線を越えたプロセスレベルの連携のためのソリューションを，たとえば共同で使用するプラットフォームを通じるなどの形で見極めることが必要不可欠となり，中立の立場からのインシデント解析やその識別およびドキュメンテーションを可能にするソリューションが求められる。

セキュリティ管理が軌道に乗って初めて，透過性の達成や異常検出，ドキュメンテーションなどの措置という形で，生産全域にわたりセキュリティ向上に自ら貢献できるようになる。

7.5.7 アウェアネス

そしてさらに必要不可欠なのは，従業員と経営陣がITセキュリティの重要性と，データの喪失や改ざんなどの深刻さを認識し，その結果としてITセキュリティの規則を理解してそれを守ることである。認識不足はセキュリティ対策を意図的にかいくぐるような行為にまでつながりかねない。セキュリティ対策によって手間が増えたり時間が余計にかかったりすることも多いからである。したがって全社員を対象に定期的な訓練および教育を実施することも重要な措置である。

7.5.8 企業全体を網羅

しかしITセキュリティはなにも製造だけの話ではない。すでに生産用コンポーネントの計画および調達の時点から始まっているのである。生産用の安全なIT環境を構築するには，計画・調達・製造の緊密な連携が必要である。調達した製品がITセキュリティの規則に技術的に対応していなければ，その規則は守りようがない。調達する製品に要求される技術的条件を知るためには，製造・計画・購買の対話が必要である。顧客が具体的な条件をつけない限り，製造者はまずセキュリティ機能を製品に実装しようとは考えない。製造費の増加につながったり，性能の低下を招くことがあるからである。製造者が対応した製品を提供しようとしなければ，市場にはあたかも他に選択肢がないかのような状況に顧客は直面することになる。このような悪循環のせいで，現在のところ製造者の製品へのITセキュリティ実装が遅々として進まないのである。このため，調達ガイドラインに規定されている製造者の製品に対する最低要求条件を定期的に改訂し適応させることが望ましい。

以上紹介した模範対策はどれも，企業内のITセキュリティを段階的に改善してゆくためのものである。これらの対策の中のどれを採用するのが具体的な事例において有意義であるかは，その事例に即して考案するのが望ましいし，それが必要でもある。また，ベストプラクティスを参考にすることもできる。

7.6 展望と要求事項

インダストリー4.0は企業の境界線を越えてオフィスからセンサまで情報の世界をひとつに結びつける。これらの情報の世界の安全は，情報処理と情報セキュリティの責任がオフィスITとオートメーションの間で分離されていることの多い現在の状況を解消することによってはじめて確保される。

現在すでにオフィスITの分野では標準および規格が存在し，情報セキュリティ（ISO 27000シリーズ）に始まり，インフラストラクチャ管理（ITIL）からビジネスに関連するIT対策（Cobit）まで多数の項目を規定している。

自動化技術の分野では（各業界独自の推奨事項[16]は多数あるものの）「情報セキュリティ」というテーマについて問題意識やリスクの認識，セキュリティ対策の具体化という点で大幅に遅れをとっている。

当面はドイツ語のVDIガイドライン2182を産業オートメーションにおける情報セキュリティの手順モデルとして利用することができる。製造者・インテグレーター・運用者の連携を考慮している。

あらゆる企業ネットワークの融合が進み，さらには価値ネットワークがまるまる一体化する一方で，さまざまなセキュリティの要件と方式が収束に向かう中，セキュリティ対策を企業全体およびサービス業者との間で調整し調和していくことが決定的に重要性をもつ。現在まだ作業中のIEC62443[17]には，管理ITの手順モデルと対策（ISO 27000シリーズ）をオートメーションの特殊性（ISA-99[18]を基盤とする）と効果的かつ安全に結びつけるという目的がある。インダストリー4.0のための新たな要求条件および対策は適宜規格として明文化する必要がある。そのために新しい規格を制定するか，それとも既存の規格の改訂および補足が好ましいかは，インダストリー4.0に関係する他の規格化項目の文脈においても評価が必要である。

ここで調和化というのは，オフィスITの安全管理と自動化技術の安全管理が歩み寄らなくてはならないということも意味する。そのために必ずしも「双方」が動く必要はない。

オートメーションの分野には，オフィスITにまったく対応するものがない指令があることは，機械指令2006/42/ECの例が示している。これは欧州レベルでの人間および環境の保護のための規制の枠組である。インダストリー4.0の動的な価値ネットワークにおいて安全操業と信頼性の確保に加え，危険のない機能をも保証することが，機械指令改訂作業での大きな課題となる。

マッチするコンポーネントを用いて危険のない機能を保証するためには，適切な統合対策および統合検証が必要である。情報セキュリティについていえば，目標とするセキュリティ水準を達成し，動的に変化する価値ネットワークでもその水準を維持するのに適した方法やメカニズムを開発する必要がある。

信頼できる認証局と一意的で偽造防止対策を施したアイデンティティの確立が，参加ユーザーの一意的かつ整合のとれた識別とアイデンティティの関連付けを確実に行い，アイデンティティに基づいた認証および権限付与をサポートする価値ネットワークに沿ったアイデンティティインフラストラクチャ構築の前提条件となる。

セキュリティが製品誕生プロセスに統合された要素になる必要がある（セキュリティバイデザイン）。

具体的な要求条件や環境条件が分野によって異なる可能性があっても，共通の手法やコンセプトで対応することは可能である。オフィスITとオートメーションの分野のノウハウを結集することで大きなシナジー効果が得られる。

16 ISA99, NIST SP800-82, NERC CIP, CPNI Good Practice Guideなど（すべて英語版）

17 https://www.dke.de/DE/STD/INDUSTRIE40/Seiten/IEC62443.aspx 参照

18 https://www.isa.org/isa99/ 参照

そのためにはオートメーションにおける要求条件に対してもその内容を広げてゆくことや，さらなる教育がオフィスIT側で必要となる一方で，オートメーション側ではITおよび特にセキュリティのノウハウを強化する必要がある。

セキュリティを取り巻く状況が静止することはあり得ない。脅威は常に変化してゆく。よってセキュリティは必ず継続的プロセスとして認識するべきであり，期限付きのプロジェクトと考えられるのはせいぜい最初のうちだけである。関係者が皆それぞれ新たなセキュリティの課題に対応する方法を見出す必要がある。製品開発や運転開始の時点では未知であった課題もある。

大きな課題は，その具体化にあたって中小企業のニーズを考慮することである。提供される製品やサービス自体に標準化されたセキュリティ特性が備えられており，それを事業プロセスに容易に組み込むことができる適切なインフラが存在してはじめて，しっかりとしたセキュリティの土壌が醸成される。そのためのステップとして考えられるのが，オートメーション製品の通信・セキュリティデータシートの統一と，セキュリティイベントに関するメッセージを統一したセマンティックスにより標準化することで，集中型の収集および解析を容易にすることなどである。

新しい価値ネットワークにおいては，情報とネットワーキングが最も重要な財となる。情報の共有や提供を通じて新たな可能性が生み出される。当然それと同時に該当する情報の所有権の問題や，当事者の役割と法的安定性のある責任分担の問題が浮上してくる。提携先や納入業者のところで情報の解析を行うことによって得られる付加価値とノウハウ流出の危険性との比較衡量が必要となる。

参考資料

8 参考資料

8.1 参考文献一覧

[1] VDI/VDE-測定・自動化技術協会；ステータスレポート；インダストリー4.0；価値連鎖，デュッセルドルフ：VDI（社），2014年4月

[2] VDI/VDE-測定・自動化技術協会；ステータスレポート；インダストリー4.0；オブジェクト，エンティティ，コンポーネント，デュッセルドルフ：VDI（社），2014年4月

[3] 未来プロジェクト・インダストリー4.0実現のための対策推奨事項；通信後援者グループ報告書，インダストリー4.0研究会最終報告書，http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf

[4] IEC TR62794:Industrial-process measurement, control and automation - Reference model for representation of production facilities (Digital Factory), 2012

[5] IEC CD 62832 Digital Factory

[6] IEC 61987-10

[7] GMA 定義：http://www.iosb.fraunhofer.de/servlet/is/48960/

[8] 連邦情報工学安全庁：2014年ドイツ国内のITセキュリティ状況，https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?blob=publicationFile

[9] www.iosb.fraunhofer.de/?BegriffeI40

[10] https://www.dke.de/de/std/informationssicherheit/documents/nr%20industrie%204.0.pdf

[11] http://docs.oracle.com/javase/7/docs/technotes/guides/jar/jar.html#JAR_Manifest

[12] http://www.plattform-i40.de/sites/default/files/140326_Broschuere_Industrie_0.pdf

8.2 インダストリー4.0用語集

インダストリー4.0では生産関連用語とICT（情報通信技術）用語が入り交じってひとつになる。しかし，過去の経緯があって，インダストリー4.0に関連する重要な用語に違いがあったり，明確でない部分も存在する。専門委員会VDI/VDE-GMA 7.21「インダストリー4.0」内に設けられたフラウンホーファーIOSB研究所のミリアム・シュレイペン工学博士を座長とする作業部会「用語」では，インダストリー4.0の共同の「基盤」（用語法）を，言語および概念の理論的骨組みとして策定する努力をしている。その作業はまたDKEの第9専門部局でこの問題を担当する各委員会（DKE/UK 921.1など）との緊密な協力のもとで進められており，プラットフォーム・インダストリー4.0の第2作業部会「リファレンスアーキテクチャ」とも調整が行われている。

基本的な用語の認識を共有するのがその目的である。ICTおよび生産の分野にすでに存在する規格および標準がその出発点となる。

インダストリー4.0に関しては，さまざまな領域の用語が取り入れられている（たとえばICT分野から取り入れられたサービス指向環境におけるサービスのオーケストレーションといった表現）。しかし，用語の中には，領域によって意味合いの異なるものもある（たとえばICTでいうサービスは生産とは違う）。同じ領域内でさえ多義であったり，厳密な意味が不明な用語もある（たとえばコンポーネント）。このような言語上および概念上の差異や不明確さ，さらには「専門外コンセプト」に関する説明の必要性などが，インダストリー4.0のための横断的かつ複雑な技術ソリューションの開発と規格化の障害となっている。

すなわちこの用語集は，さまざまな観点や要求条件を考慮したインダストリー4.0関連用語の共通基盤を整備するためのものである。これにより企業と業種の境界線を越えた連携を促進するのが目的であり，これはまた規格化を進めるための前提条件でもある。

現在の定義は[9]に記載されている。

8.3 執筆チーム

本実現戦略への内容的インプットはプラットフォーム・インダストリー4.0の各作業部会において作成した。以下に記載するのは，その内容を書面として本報告書にまとめた著者たちである。

執筆チーム　1章～4章：

- Wolfgang Dorst (BITKOM e.V.)
- Carsten Glohr (Detecon International GmbH)
- Thomas Hahn (Siemens AG)
- Frank Knafla (Phoenix Contact Electronics GmbH)
- Dr. Ulrich Loewen (Siemens AG)
- Roland Rosen (Siemens AG)
- Thomas Schiemann (T-Systems International GmbH)
- Friedrich Vollmar (IBM Deutschland GmbH)
- Christoph Winterhalter (ABB AG)

執筆チーム　5章：

- Dr. Bernhard Diegner (ZVEI e.V.)
- Johannes Diemer (Hewlett Packard GmbH)
- Dr. Mathias Dümmler (Infineon Technologies AG)
- Stefan Erker (Huber + Suhner GmbH)
- Dr. Werner Herfs (RWTH Aachen, WZL - Lehrstuhl für Werkzeugmaschinen)
- Claus Hilger (HARTING IT Services GmbH & Co. KG)
- Dr. Lutz Jänicke (Innominate Security Technologies AG)
- Prof. Dr.-Ing. Jürgen Jasperneite (Institut für industrielle Informationstechnik / inIT, Hochschule OWL, Lemgo und Fraunhofer IOSB-INA)
- Johannes Kalhoff (Phoenix Contact GmbH & Co. KG)
- Prof. Dr. Uwe Kubach (SAP AG)
- Dr. Ulrich Löwen (Siemens AG)
- Georg Mattis (Huber + Suhner GmbH)
- Georg Menges (NXP Semiconductors Germany GmbH)
- Frank Mildner (Deutsche Telekom AG)
- Mathias Quetschlich (MAN Truck & Bus AG)
- Ernst-Joachim Steffens (Deutsche Telekom AG)
- Dr. Thomas Stiedl (Robert Bosch GmbH)

執筆チーム　6章：

- Dr. Peter Adolphs (Pepperl+Fuchs GmbH)
- Dr. Heinz Bedenbender (VDI e.V.)
- Martin Ehlich (Lenze SE)
- Prof. Ulrich Epple (RWTH Aachen)
- Martin Hankel (Bosch Rexroth AG)
- Roland Heidel (Siemens AG)
- Dr. Michael Hoffmeister (Festo AG & Co.KG)
- Haimo Huhle (ZVEI e.V.)
- Bernd Kärcher (Festo AG & Co.KG)
- Dr. Heiko Koziolek (ABB AG)
- Reinhold Pichler (VDE e.V. DKE)
- Stefan Pollmeier (ESR Pollmeier GmbH)
- Frank Schewe (Phoenix Contact Electronics GmbH)
- Thomas Schulz (GE Intelligent Platforms GmbH)
- Dr. Karsten Schweichhart (Deutsche Telekom AG)
- Dr. Armin Walter (Lenze SE)
- Bernd Waser (Murrelektronik GmbH)
- Prof. Dr. Martin Wollschlaeger (TU Dresden)

執筆チーム　7章：

- Dr. Lutz Jänicke (Innominate Security Technologies)
- Michael Jochem (Bosch Rexroth AG)
- Hartmut Kaiser (Secunet Security Networks AG)
- Marcel Kisch (IBM Deutschland GmbH)
- Dr. Wolfgang Klasen (Siemens AG)
- Jörn Lehmann (VDMA e.V.),
- Lukas Linke (ZVEI e.V.)
- Jens Mehrfeld (BSI)
- Michael Sandner (Volkswagen AG)