第五次産業革命（インダ33ストリー5.0）とサイバーセキュリティの変革：人間中心・持続可能・レジリエントな未来への戦略的考察

2025年4月18日
生成AIを利用して作成
中山　正樹　編集

エグゼクティブサマリー

第五次産業革命、すなわちインダストリー5.0は、2021年に欧州委員会によって提唱された産業変革の新たなビジョンである[1]。これは、効率性と生産性のみを追求したインダストリー4.0のパラダイムを補完し、産業が社会により広範な価値を提供することを目指すものである[3]。インダストリー5.0は、「人間中心（Human-Centric）」「持続可能性（Sustainability）」「回復力（Resilience）」という三つの柱を核とし、労働者の幸福を生産プロセスの中心に据え、地球環境の限界を尊重しながら、技術革新を通じて繁栄を追求する[1]。

インダストリー4.0が自動化とコネクティビティに主眼を置いたのに対し、インダストリー5.0は人間と機械の協働（Human-Machine Collaboration: HMC）を重視し、人間の創造性や批判的思考といった独自の能力を技術によって増強することを目指す[5]。この変革は、AI、IoT、ビッグデータ、協働ロボット（Cobot）、サイバーフィジカルシステム（CPS）、デジタルツインといった先進技術によって支えられている[8]。

しかし、この高度な相互接続性と人間と機械の融合は、サイバーセキュリティに新たな、そして深刻な課題をもたらす。攻撃対象領域は、ITシステムからOT（Operational Technology）システム、IoTデバイス、協働ロボット、さらにはサプライチェーン全体へと劇的に拡大する[11]。AIを利用した高度な攻撃、HMC環境における安全とセキュリティの融合リスク、OTシステムへの侵入、サプライチェーンを通じた脅威の拡散などが、新たな脅威として顕在化している[11]。

これらの脅威に対抗するため、サイバーセキュリティ戦略は根本的な変革を迫られている。境界防御モデルはもはや有効ではなく、「決して信頼せず、常に検証する」ゼロトラストアーキテクチャの導入が不可欠となる[15]。AIを活用した防御（AI-Driven Defense）は、高度化する脅威をリアルタイムで検知・対応するために必須であり、OTセキュリティの強化、サプライチェーン全体のセキュリティリスク管理（SCRM）も急務である[17]。さらに、インダストリー5.0の人間中心の理念に基づき、ユーザビリティを考慮した「人間中心のセキュリティ設計」と、従業員のセキュリティ意識向上が求められる[20]。

データプライバシーと倫理も重要な課題である。HMCやAIによるパーソナライズが進む中で生成される膨大なデータの管理、GDPR（EU一般データ保護規則）などの規制遵守、AIのバイアスや透明性といった倫理的問題への対応が不可欠となる[22]。

将来を見据え、組織はこれらの変化に対応するための包括的なサイバーセキュリティロードマップを策定する必要がある。これには、技術導入、人材育成（IT/OT/安全/人間工学の融合スキル）、プロセス適応、そして経営層のリーダーシップに基づくガバナンス強化が含まれる[25]。インダストリー5.0が目指す、人間中心で持続可能、かつレジリエントな産業の未来を実現するためには、サイバーセキュリティを単なる技術的課題ではなく、信頼構築と事業継続のための戦略的基盤として位置づけることが不可欠である。

1. 第五次産業革命（インダストリー5.0）の定義：次なる産業進化

1.1 起源と公式定義

第五次産業革命、一般に「インダストリー5.0」として知られる概念は、2021年1月に欧州委員会（European Commission）によって正式に提唱された、産業界における次世代の変革ビジョンである[1]。この概念は、単なる技術革新の段階を示すだけでなく、産業が社会全体に対して果たすべき役割を再定義しようとする試みである。

欧州委員会の公式な定義によれば、インダストリー5.0は「効率性と生産性を唯一の目標とする考え方を超え、社会に対する産業の役割と貢献を強化する」ビジョンを提供する[3]。具体的には、「労働者の幸福（wellbeing）を生産プロセスの中心に置き、地球の生産限界を尊重しながら、雇用と成長を超えた繁栄を提供するために新しい技術を使用する」ことを目指している[3]。重要な点として、インダストリー5.0は、先行するインダストリー4.0（第四次産業革命）を置き換えるものではなく、むしろそれを補完し、拡張する位置づけにある[31]。インダストリー4.0がもたらしたデジタル化や自動化の基盤の上に、人間的、社会的、環境的な側面を統合しようとするものである。

インダストリー5.0の提唱背景には、インダストリー4.0の推進によって顕在化した課題への対応という側面がある[34]。技術中心の効率化追求が、労働者の役割や幸福、環境への配慮といった側面を十分にカバーできていないとの認識が広がった。さらに、気候変動、資源枯渇、そして新型コロナウイルス感染症（COVID-19）のパンデミックや地政学的な変動といった世界規模の課題が、従来の産業モデルの脆弱性を露呈させた[4]。これらの経験から、変化に対する「回復力（レジリエンス）」の重要性が強く認識され、インダストリー5.0の重要な柱の一つとして位置づけられることとなった。

1.2 中核となる三つの柱

インダストリー5.0は、以下の三つの相互に関連する中核的な柱（キーコンセプト）に基づいている[1]。

- 人間中心（**Human-Centric**）:
    - 定義: この柱は、生産活動の中心に人間、すなわち労働者のニーズ、関心、幸福、スキルを据えることを最優先する考え方である[1]。技術は人間を置き換えるためではなく、人間を支援し、その能力を強化するために活用されるべきであるという思想に基

づいている[5]。技術は労働者のニーズや多様性に適応すべきであり、その逆ではない[32]。
    - 含意: 人間中心アプローチは、単なる労働力の提供者としてではなく、創造性、批判的思考、複雑な問題解決能力といった人間固有のスキルを尊重し、活用することを目指す[1]。機械との協働（HMC）を通じて、危険な作業や単調な作業から人間を解放し、より付加価値の高い、創造的な業務への集中を促す[6]。これにより、労働者のエンパワーメント、スキルの向上（アップスキリング/リスキリング）、多様性の促進が図られる[4]。究極的には、労働者の安全と幸福感を高め、より魅力的で働きがいのある職場環境を創出することを目指す[3]。EU産業界におけるスキルギャップの解消も重要な目的の一つである[4]。
- 持続可能性（**Sustainability**）:
    - 定義: この柱は、産業活動が地球環境の限界内で営まれること、すなわち「惑星の境界（planetary boundaries）」を尊重することを要求する[1]。経済的価値の追求と同時に、環境的・社会的責任を果たすことが不可欠であるという認識に基づいている。欧州グリーンディールのような政策目標とも強く連携している[4]。
    - 含意: 持続可能性の追求は、資源効率の向上、廃棄物の削減、循環型経済モデル（リユース、リサイクル）への移行を促進する[4]。具体的には、再生可能エネルギーの利用拡大、製品ライフサイクル全体での環境負荷低減、CO2排出量の削減（カーボンニュートラルな製造プロセスの開発など）といった取り組みが含まれる[29]。これにより、将来世代への負担を残さない形で産業を発展させ、気候変動対策や資源保全といった地球規模の課題解決に貢献することが期待される[4]。
- 回復力（**Resilience**）:
    - 定義: この柱は、パンデミック、自然災害、地政学的変動、供給網の途絶といった予期せぬ破壊的な変化や危機（ショック）に対して、産業基盤や社会生活を保護し、迅速に回復・適応する能力を強化することを目指す[1]。
    - 含意: レジリエンスの強化には、産業プロセスやサプライチェーンにおける俊敏性（Agility）と適応性（Adaptability）が求められる[6]。具体的には、柔軟な生産システム、適応可能な技術の導入、戦略的なバリューチェーンの見直し、エネルギー消費慣行の再考などが挙げられる[4]。また、サプライチェーンの脆弱性を低減するために、生産拠点の分散化や地域内での生産（ローカライゼーション）といった動きも含まれる可能性がある[6]。サイバーセキュリティの確保は、外部からのサイバー攻撃というショックに対する耐性を高める上で、レジリエンス構築の重要な要素となる[4]。

1.3 焦点の転換：効率性から社会的価値と労働者の幸福へ

インダストリー5.0は、インダストリー4.0でしばしば最優先された株主価値（Shareholder Value）の最大化という視点から、労働者、社会、環境を含むより広範なステークホルダー（Stakeholder）全体の価値創造へと焦点を移行させる[32]。産業は単に雇用と経済成長を生み出すエンジンであるだけでなく、気候変動、資源保全、社会的安定といった現代社会が直面す

る課題に対する解決策を提供する存在（プロバイダー）として位置づけられる [3]。

この価値観の転換は、インダストリー5.0の根幹をなす重要な変化である。特に、「回復力（レジリエンス）」が中核的な柱として明示的に組み込まれた点は注目に値する。これは、近年のパンデミックや地政学的な混乱といったグローバルなショック [4] を通じて、インダストリー4.0が追求してきた高度な最適化やグローバルに分散したサプライチェーン [7] が持つ固有の脆弱性が明らかになったことへの直接的な応答である。インダストリー4.0における「効率性至上主義」とも言える側面に対し、インダストリー5.0は、ストレス下においても事業継続性を確保できるような適応性と頑健性をバランス良く追求するモデルへの移行を促している。

このレジリエンスの重視は、サイバーセキュリティの戦略的重要性にも直接的な影響を与える。サイバー攻撃は現代における主要な事業中断要因の一つであり、産業インフラやサプライチェーンの機能を麻痺させる可能性があるため、レジリエンスとサイバーセキュリティは本質的に結びついている [20]。したがって、インダストリー5.0においてレジリエンスが中核的な柱として格上げされたことは、サイバーセキュリティを単なるコストセンターや技術的な防御策としてではなく、新たな産業パラダイムの核心目標を達成するための戦略的な必須要件へと昇格させることを意味する。

2. インダストリー5.0 vs. インダストリー4.0：比較分析

2.1 革命ではなく進化：インダストリー4.0の基盤の上に

インダストリー5.0は、第四次産業革命（インダストリー4.0）を否定し、置き換えるものではない点を理解することが重要である [31]。むしろ、インダストリー4.0が築き上げた技術的基盤、すなわちIoT（モノのインターネット）、AI（人工知能）、ビッグデータ分析、サイバーフィジカルシステム（CPS）、自動化技術などを継承し、その上に構築される進化形と捉えるべきである [7]。

インダストリー5.0は、インダストリー4.0の実装過程で見られた限界や潜在的な負の側面に対応する形で構想された側面を持つ [34]。例えば、完全自動化による雇用喪失への懸念、技術中心主義が行き過ぎて人間的側面や社会的・環境的ニーズへの配慮が不足する可能性などが指摘されてきた [20]。インダストリー5.0は、これらの課題に対処し、よりバランスの取れた、持続可能な産業のあり方を提示しようとしている。

2.2 主要な差別化要因：目標、技術、そして人間の役割

インダストリー4.0と5.0の最も顕著な違いは、その目指す方向性、重点を置く技術、そして生産プロセスにおける人間の位置づけにある。

- **目標:** インダストリー4.0の主たる目標は、多くの場合、効率性、生産性、自動化レベルの向上、コスト削減、そしてスマートファクトリーにおける高度なコネクティビティの実現にあった [4]。これに対し、インダストリー5.0はこれらの目標を包含しつつも、さらに人間の幸福（ウェルビーイング）、社会的価値の創出、環境持続可能性、危機に対する回復力（レ

ジリエンス）、そして高度なパーソナライゼーション（個別化）やカスタマイゼーションを中核的な達成目標として掲げている[1]。

- 技術的焦点: インダストリー4.0は、プロセスの最適化と自動化を目的として、IoT、CPS、ビッグデータ、AIといった技術の活用を強調した[7]。インダストリー5.0もこれらの技術を活用するが、特に人間と機械の効果的な協働（HMC）を可能にする技術（協働ロボット（Cobot）、AR/VR、高度なHMI）、個別化生産を実現する技術（アディティブ・マニュファクチャリング/3Dプリンティング）、そして持続可能性に貢献する技術（スマートマテリアル、バイオテクノロジー、エネルギー効率化技術）に重点を置いている[5]。
- 人間の役割: インダストリー4.0のアプローチは、しばしば人間のタスクを自動化することを目指し、結果として労働力の削減や、人間が機械を監視する役割へと変化する可能性を示唆していた[7]。対照的に、インダストリー5.0は明確に人間を「中心」に据える[1]。人間は機械と「協働」するパートナーであり、その創造性、批判的思考、問題解決能力といった機械にはない独自のスキルが最大限に活用される[5]。労働者のエンパワーメント、スキルアップ、そして安全で健康的な労働環境の提供が重視される[1]。日本政府が提唱する「Society 5.0」もこの人間中心のアプローチを共有しているが、その適用範囲は産業界に留まらず、社会全体へとより広範である[1]。

2.3 特徴比較表：インダストリー4.0 vs. インダストリー5.0

インダストリー4.0から5.0への進化における主要な違いを明確にするため、以下の比較表を提示する。この表は、両者の核心的な差異を構造化し、戦略的な理解を助けることを目的とする。

特徴次元	インダストリー4.0 (第四次産業革命)	インダストリー5.0 (第五次産業革命)
主たる目標	効率性、生産性向上、自動化、コスト削減、スマートファクトリー化[4]	人間の幸福、社会的価値創出、持続可能性、回復力（レジリエンス）、高度な個別化[3]
人間の役割	機械の監視者、自動化による代替の可能性、効率化のための要素[7]	生産プロセスの中心、機械との協働者、創造性・判断力の活用、エンパワーメントの対象[4]
技術的重点	IoT、CPS、ビッグデータ、AIによる自動化・最適化、コネクティビティ[7]	人間機械協働（HMC）技術（Cobot, AR/VR, HMI）、個別化技術（3Dプリンティング）、持続可能性技術、レジリエンス支援技術（デジタルツイン等）[6]

中核となる柱/価値	暗黙的：効率性、接続性、データ駆動	明示的：人間中心、持続可能性、回復力 [1]
推進力	技術主導（テクノロジー・プッシュ）、効率化への要求	価値主導（バリュー・ドリブン）、社会的・環境的要請（ソシエタル・プル） [31]

この比較表は、インダストリー5.0が単なる技術的な進歩ではなく、産業の目的や価値観そのものに関する根本的な転換を含意していることを示している。

3. インダストリー5.0の技術的基盤

インダストリー5.0のビジョンを実現するためには、インダストリー4.0から引き継がれ、さらに発展した多様な技術群が不可欠な役割を果たす。これらの技術は相互に連携し、人間中心、持続可能性、回復力という目標達成を支える。

3.1 AI、IoT、ビッグデータ分析における相乗効果

AI（人工知能）、IoT（モノのインターネット）、そしてビッグデータ分析は、インダストリー4.0の中核技術であったが、インダストリー5.0においてもその重要性は変わらず、むしろその活用範囲と深化が求められる [1]。

インダストリー5.0におけるこれらの技術の役割は多岐にわたる。IoTデバイス（センサー、アクチュエーター等）が収集した膨大なリアルタイムデータを、クラウドやエッジでAIが分析し、ビッグデータとして蓄積・活用する [7]。これにより、以下のような機能が実現される。

- インテリジェントな自動化: 単純な自動化を超え、状況に応じて自律的に判断・動作する高度な自動化。
- リアルタイム監視と予知保全: 設備やプロセスの状態を常時監視し、AI分析によって故障や異常の兆候を事前に検知し、計画的なメンテナンスを可能にする [6]。
- データ駆動型の意思決定支援: 人間のオペレーターや管理者に対し、AIが分析結果や予測情報を提供し、より迅速かつ的確な意思決定を支援する [1]。
- 持続可能性のための最適化: エネルギー消費量や資源使用量を監視・分析し、無駄を削減するためのプロセス最適化を支援する [36]。
- 人間機械協働（HMC）の実現: AIが人間の意図を理解したり、ロボットの動作を制御したりすることで、スムーズで安全な協働を可能にする [5]。特に、生成AI（Generative AI）は、人間の認知能力を拡張し、企業内での情報検索（スマートサーチ）などを効率化する可能性を秘めている [74]。

3.2 協働ロボット（Cobot）と先進ロボティクスの台頭

インダストリー5.0の人間中心アプローチを象徴する技術の一つが、協働ロボット（Cobot）であ

る[5]。Cobotは、従来の産業用ロボットが安全柵などで人間から隔離された環境で動作していたのとは異なり、高度なセンサーや制御技術によって、人間と同じ作業空間で安全に隣り合って働くことができるように設計されている[66]。

Cobotの主な役割は、人間が行うには反復的、精密すぎる、あるいは身体的負担が大きいタスク（組立、ピッキング、研磨、塗装、検査、梱包、機械への部品供給、危険物取り扱いなど）を代替または補助することである[6]。これにより、人間はより複雑な判断、創造的な問題解決、品質管理、プロセスの監督といった、人間ならではの能力が求められる業務に集中できるようになる[49]。

Cobot導入によるメリットは多岐にわたる。生産性の向上はもちろんのこと、製品品質の安定化、作業の柔軟性向上（多品種少量生産への対応など）、労働力不足の解消、そして何よりも作業者の安全性向上と身体的・精神的負荷の軽減（人間工学的改善）に貢献する[1]。

3.3 サイバーフィジカルシステム（CPS）とデジタルツインの役割

サイバーフィジカルシステム（CPS）は、計算能力（サイバー）と物理的なプロセス（フィジカル）を緊密に統合するシステムであり、インダストリー4.0および5.0の根幹をなす概念である[9]。物理世界の出来事をセンサー等でデジタルデータとして捉え、それを分析・処理し、その結果に基づいて物理世界のアクチュエーター等を制御するというループを形成する。

このCPSの能力を飛躍的に高めるのが、デジタルツイン（DT）である[1]。デジタルツインとは、物理的な資産（機械、製品、工場ライン、プロセス全体など）の仮想的なレプリカ（双子）をデジタル空間上に構築し、現実世界のIoTセンサーなどから送られてくるリアルタイムデータと連携させる技術である。

インダストリー5.0において、デジタルツインは以下のような多様な目的で活用される。

- **シミュレーションと最適化:** 実際の設備を動かす前に、仮想空間上で様々なシナリオをシミュレーションし、プロセスの最適化、ボトルネックの特定、新製品導入の影響評価などを行う[1]。
- **予知保全とリスク評価:** リアルタイムデータに基づき、設備の劣化状況や故障の可能性を予測し、メンテナンス計画を最適化する[6]。サイバーセキュリティリスクの評価にも応用可能である。
- **人間機械協働（HMC）の強化:** HMCワークスペースのデジタルツインを作成し、タスクの計画、シミュレーション、最適化、リアルタイムでの状況認識共有などを支援する[41]。特に、人間中心のデジタルツイン（Human Digital Twin: HDT）は、人間の状態（疲労度、認知負荷など）もモデル化し、より安全で効率的な協働を実現する鍵となる[41]。
- **トレーニングとスキル開発:** 仮想環境での操作訓練や緊急時対応訓練を安全に行うことができる[43]。
- **持続可能性とレジリエンスの向上:** エネルギー消費や資源利用のシミュレーションによる

効率化、サプライチェーンの脆弱性分析などに活用される[7]。

3.4 インターフェースを通じた人間機械協働（HMC）の強化（AR/VR）

人間と機械が効果的に協働するためには、両者間の円滑なコミュニケーションと情報共有を可能にするインターフェースが不可欠である。直感的で使いやすい人間機械インターフェース（Human-Machine Interface: HMI）の設計が重要となる[6]。

特に、拡張現実（Augmented Reality: AR）と仮想現実（Virtual Reality: VR）は、インダストリー5.0におけるHMCを大きく前進させる可能性を秘めている[5]。

- **AR:** 現実世界の視界にデジタル情報を重ねて表示する技術。作業者に対して、リアルタイムでの作業指示、部品情報の表示、遠隔からの専門家による指示などを提供し、複雑な組立作業やメンテナンス作業の効率と精度を向上させる[5]。
- **VR:** 完全な仮想空間を生成する技術。没入感の高いトレーニング環境の提供（安全な緊急時対応訓練など）、製品設計のレビュー、遠隔地との共同作業などに活用される[43]。

これらの技術は、作業者が必要な情報を適切なタイミングと形式で受け取ることを可能にし、認知負荷を軽減し、より安全で効率的な作業遂行を支援する。AR/VR技術のさらなる統合は、今後の重要なトレンドと目されている[58]。

3.5 支援技術：クラウド、エッジ、アディティブ・マニュファクチャリング、バイオテクノロジー等

上記の主要技術に加え、インダストリー5.0の実現には以下のような支援技術も重要な役割を担う。

- クラウドコンピューティング**:** 大規模なデータストレージ、高度な計算能力を提供し、ビッグデータ分析やAIモデルの学習・実行基盤となる[7]。
- エッジコンピューティング**:** データが発生する現場（エッジ）に近い場所でデータ処理を行う技術。リアルタイム性が要求される制御やHMC、大量のIoTデータを効率的に処理するために不可欠であり、遅延を削減し、ネットワーク帯域への負荷を軽減する[7]。
- アディティブ・マニュファクチャリング（**3D**プリンティング）**:** 材料を積層して立体物を造形する技術。高度なカスタマイゼーション、少量生産、ラピッドプロトタイピング、軽量かつ高強度な部品の製造、さらには生産拠点の分散化（ローカライズド生産）を可能にする[43]。
- バイオテクノロジーとスマートマテリアル**:** 生物由来の持続可能な新素材の開発、自己修復機能を持つ材料、環境負荷の少ない製造プロセス、埋め込みセンサーを持つスマート材料など、持続可能性と機能性向上に貢献する[9]。
- ブロックチェーン**:** サプライチェーンにおけるトレーサビリティ向上、データの透明性と改ざん防止、セキュアな取引記録などに活用される可能性がある[10]。
- 先進的ネットワーク（**5G/6G**）**:** 超高速、低遅延、多数同時接続といった特徴により、膨大な数のIoTデバイスの接続、リアルタイム制御、遅延が許されないHMCアプリケーションなどを実現するための通信基盤を提供する[6]。

これらの多様な技術（AI、IoT、Cobot、DT、AR/VR、エッジ、クラウド、アディティブ・マニュファクチャリング等）が組み合わさり、相互に連携することで、インダストリー5.0は前例のないほど複雑で相互接続された技術エコシステムを形成する。この複雑性は、単に構成要素が増えるだけでなく、それらの間の相互作用、依存関係、そして潜在的な脆弱性という観点から、指数関数的に増大する。例えば、IoTセンサーからのデータがデジタルツインやAIモデルの精度を左右し、AIの判断がCobotの動作を制御し、そのすべてがエッジやクラウド、5G/6Gネットワークに依存するといった具合である [7]。

このような複雑な網の目を管理し、保護するためには、個々の技術に対するサイロ化されたセキュリティ対策（例えば、ネットワークファイアウォール、データ暗号化）だけでは不十分である。システム全体を俯瞰し、構成要素間の相互作用や依存関係から生じるリスクを理解し、管理する、ホリスティックな、システム思考に基づいたアプローチが不可欠となる。一つのコンポーネントの脆弱性が、連鎖的にシステム全体に影響を及ぼす可能性 [12] を常に考慮に入れなければならない。

4. インダストリー5.0がサイバーセキュリティの脅威状況に与える影響

インダストリー5.0への移行は、生産性、持続可能性、労働者の幸福といった面で大きな利益をもたらす一方で、サイバーセキュリティの脅威状況を根本的に変化させ、新たなリスクを生み出す。高度な相互接続性、人間と機械の融合、そしてITとOTの境界の曖昧化は、攻撃者にとって新たな機会を提供することになる。

4.1 拡大する攻撃対象領域：ハイパーコネクティビティのリスク

インダストリー5.0環境は、本質的にハイパーコネクテッドである。工場内の機械、センサー、アクチュエーター、協働ロボット（Cobot）、ウェアラブルデバイスといった無数のIoTデバイスがネットワークに接続される [11]。さらに、これらのデバイスやシステムは、エッジコンピューティングノード、クラウドプラットフォーム、サプライヤーや顧客のシステムとも連携する [21]。この結果、サイバー攻撃者が侵入を試みることができる潜在的なエントリーポイント、すなわち「攻撃対象領域（Attack Surface）」が劇的に拡大する [11]。

特に深刻なのは、従来は比較的隔離されていたOT（Operational Technology）システム、すなわち産業制御システム（ICS）が、IT（Information Technology）ネットワークやインターネットに接続される機会が増えることである [16]。これにより、企業のオフィスネットワークへの侵入が、工場ラインの停止や物理的な損害を引き起こすOTシステムへの攻撃へと波及する経路が生まれやすくなる。逆に、OT環境の脆弱性を突いた攻撃が、企業の機密情報が保管されているITシステムへと侵入する足掛かりとなる可能性もある。ITとOTの境界が曖昧になることで、従来型の境界防御モデルの有効性は著しく低下する [16]。

4.2 新たな脅威と増幅される脅威

インダストリー5.0の特性は、既存のサイバー脅威を増幅させるとともに、新たな形態の攻撃を生み出す。

- 高度化するランサムウェア: 従来のデータ暗号化による身代金要求に加え、OTシステムを標的とし、生産ラインの停止や物理的な破壊を示唆して脅迫する、より悪質なランサムウェア攻撃が増加する可能性がある [11]。重要インフラへの影響は特に深刻である。
- **AIの兵器化（Weaponization of AI）:** 攻撃者もAI技術を活用し、攻撃の効率と巧妙さを高める。例えば、より説得力のあるフィッシングメールの自動生成 [11]、防御システムを回避するように自己進化するマルウェアの開発 [82]、標的の脆弱性調査の自動化、ソーシャルエンジニアリングのためのディープフェイク生成などが挙げられる [96]。さらに、産業用AIモデル自体を標的とする「敵対的攻撃（Adversarial Attack）」も懸念される。これは、AIへの入力データに微細な改変を加えることで、AIに誤認識や誤った判断を引き起こさせ、生産プロセスの混乱や品質低下を狙うものである [24]。
- **IoTデバイスの悪用:** セキュリティ対策が不十分なIoTデバイス（安価なセンサーやレガシー機器など）は、ネットワーク侵入の足掛かりとして、あるいは物理プロセスを妨害するための踏み台として悪用されやすい [11]。多数のIoTデバイスを乗っ取って形成されるボットネットは、DDoS攻撃などに利用される [100]。
- サプライチェーン攻撃: インダストリー5.0は、ハードウェア、ソフトウェア、サービスにおいて複雑なサプライチェーンに依存している。この連鎖のどこか一箇所（部品供給業者、ソフトウェア開発元、システムインテグレーターなど）が侵害されると、それが連鎖的に波及し、最終的なユーザー企業に甚大な被害をもたらす可能性がある [11]。ソフトウェアの依存関係における脆弱性（Software Dependencies）は特に重大な懸念事項であり、トップレベルの脅威として認識されている [91]。
- サービス妨害（**DoS/DDoS**）攻撃: 相互接続されたシステム群に対して大量の不正トラフィックを送りつけ、システムを過負荷状態に陥らせる攻撃。生産ラインの停止、重要サービスの提供不能などを引き起こす可能性がある [11]。インダストリー5.0の相互依存性の高さは、DDoS攻撃の影響を増幅させる。
- 中間者（**MitM**）攻撃: デバイス間、あるいは人間と機械間の通信を傍受・改ざんする攻撃。機密情報の窃取や不正なコマンドの注入につながる [13]。
- 内部脅威: インダストリー5.0では、人間がより複雑なシステムと直接的に関わる機会が増えるため、内部関係者による脅威のリスクも高まる。悪意を持った従業員による意図的な妨害行為だけでなく、操作ミスや設定不備といった意図しないヒューマンエラーが、重大なセキュリティインシデントを引き起こす可能性も増大する [12]。

4.3 基盤技術における脆弱性

インダストリー5.0を支える主要技術自体にも、固有の脆弱性が存在する。

- **AI/ML:** 訓練データへの悪意あるデータの注入（データポイズニング）、モデルからの機密情報抽出（モデルインバージョン）、前述の敵対的攻撃、アルゴリズムに内在するバイアス（公平性の問題）、判断根拠の不透明性（ブラックボックス問題）などが指摘されている

[24]。

- **HMC/Cobot:** 物理的なアクセスによる改ざん（タンパリング）がサイバーセキュリティ状態に影響を与える可能性、通信プロトコルの安全性欠如、不十分な認証メカニズム、不正な遠隔操作による乗っ取り、安全機能の意図的な無効化などがリスクとなる[14]。
- **CPS/デジタルツイン:** リアルタイムデータと仮想モデル間の同期のずれ、データの完全性（インテグリティ）の欠如、基盤となるIoT/センサーネットワークの脆弱性、仮想モデルへの不正な操作が物理的な損害を引き起こす可能性などが懸念される[12]。
- **IoT:** 初期設定のパスワードが弱い、通信が暗号化されていない、ファームウェアのアップデート機能が安全でない、物理的にアクセスしやすい場所に設置されている、といった基本的なセキュリティ対策の不備が多く見られる[11]。

4.4 IT/OTセキュリティのギャップ

前述の通り、ITとOTの融合はインダストリー5.0の重要な側面だが、両者のセキュリティに対する考え方や優先順位の違いが大きな課題となっている[16]。ITセキュリティは伝統的に機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）のCIAトライアドを重視するのに対し、OTセキュリティは安全性（Safety）と可用性（Availability）を最優先し、リアルタイム性とシステムの継続的稼働を確保することが求められる[16]。多くのOTシステムは長期間にわたって稼働するように設計されており、最新のセキュリティ機能が実装されていないレガシーシステムも少なくない[16]。

インダストリー5.0の人間中心という特性は、このIT/OT融合の課題をさらに複雑化させる。人間と協働ロボットがOT環境に直接組み込まれる[67]ことで、必要とされるセキュリティ制御（アクセス管理、脅威検知など）は、ITレベルの堅牢性を持ちつつ、同時にOT環境のリアルタイム性や人間のワークフローを阻害しない柔軟性とユーザビリティ、そして物理的な安全性を確保しなければならない。例えば、IT環境では標準的な複雑な認証プロセスも、ペースの速い生産ラインのHMIにそのまま適用すると、非実用的であるか、あるいは安全性を損なう可能性すらある。

このようなハイブリッドなIT/OT/ヒューマン環境に適したセキュリティソリューションを設計・運用するには、ITセキュリティ、OTプロセス、物理的安全、そして人間工学（ヒューマンファクター）のすべてに精通した人材が必要となる。しかし、このような複合的なスキルセットを持つ専門家は現状では非常に少なく、これがインダストリー5.0の安全な導入における深刻なボトルネックとなり得る[26]。

4.5 主要なリスクベクトルとしてのサプライチェーンの複雑性

インダストリー5.0は、ハードウェア、ソフトウェア、クラウドサービス、コンサルティングなど、多岐にわたる分野で、グローバルに展開された複雑なサプライチェーンに大きく依存している[9]。この相互接続性の高さは、効率性やイノベーションを促進する一方で、セキュリティリスクを増

大させる要因ともなっている。

サプライチェーンのいずれかの段階（例えば、部品メーカー、ソフトウェア開発ベンダー、物流業者、保守サービス提供者）でセキュリティ侵害が発生した場合、その影響は連鎖的に波及し、最終製品やサービスを利用する企業に深刻な被害をもたらす可能性がある[11]。特に、ソフトウェアコンポーネントの依存関係における脆弱性管理は、極めて重要な課題として認識されている[91]。信頼できると思われていたベンダーから提供されたソフトウェアやハードウェアに、意図的にマルウェアが埋め込まれていたり、未知の脆弱性が存在したりするリスクは、常に考慮しなければならない。

5. インダストリー5.0時代に向けたサイバーセキュリティ戦略の適応

インダストリー5.0がもたらす新たな脅威と拡大する攻撃対象領域に対応するため、従来のサイバーセキュリティ戦略は根本的な見直しと適応を迫られている。人間中心、持続可能性、回復力というインダストリー5.0の理念を実現するためには、セキュリティを後付けの対策ではなく、システム設計と運用プロセスに不可分な要素として組み込む必要がある。

5.1 ゼロトラストの必須化

従来の「城と堀」に例えられる境界防御モデル（ネットワークの内側は信頼し、外側は信頼しない）は、インダストリー5.0のような複雑で境界が曖昧な環境ではもはや有効ではない。そこで必須となるのが、「ゼロトラスト（Zero Trust）」アーキテクチャ（ZTA）の考え方である[15]。

ゼロトラストは、「決して信頼せず、常に検証する（Never Trust, Always Verify）」という原則に基づき、ネットワークの内外を問わず、いかなるユーザー、デバイス、アプリケーションからのアクセス要求に対しても、その都度厳格な認証と認可を行うセキュリティモデルである[16]。具体的には、強力なアイデンティティ認証、必要最小限の権限のみを付与する「最小権限の原則（Least Privilege）」、ネットワークを細かく分割して侵害の影響範囲を限定する「マイクロセグメンテーション」などの技術要素で構成される[93]。

インダストリー5.0環境においてゼロトラストが不可欠な理由は、多様な主体（人間、Cobot、IoTデバイス、AIエージェントなど）が複雑に連携し、従来のネットワーク境界が意味をなさなくなるためである[16]。ITとOTの融合環境においても、アクセス制御をきめ細かく行う上でゼロトラストは重要な役割を果たす[16]。

ただし、特にOT環境やHMC環境へのゼロトラスト導入には課題も存在する。リアルタイム性の要求、レガシーシステムの存在、独自の通信プロトコルなどが障壁となり得る[16]。そのため、完全なネットワークレベルでの実装だけでなく、まずはアイデンティティ管理、デバイスの健全性評価（ポスチャチェック）、アプリケーションへのアクセス制御といった側面から段階的に導入を進めるアプローチが現実的である[16]。

5.2 AI駆動型防御（AI-Driven Defense）

攻撃者がAIを活用して攻撃を高度化させる以上、防御側もAI/ML（機械学習）を駆使して対抗する必要がある[26]。AI駆動型防御は、インダストリー5.0時代のサイバーセキュリティ戦略の中核をなす要素となる。

AI/MLは、人間では処理しきれない膨大な量のセキュリティ関連データ（ログ、ネットワークトラフィック、脅威情報など）を高速に分析し、人手では見逃してしまうような異常なパターンや未知の脅威の兆候を検知する能力に優れている[17]。

具体的な応用例としては、以下のようなものが挙げられる。

- **AIを活用したセキュリティ運用（AI-SecOps）:** 脅威検知、インシデント分析、対応策の提案・自動実行などをAIが支援し、セキュリティオペレーションセンター（SOC）の効率と精度を向上させる[78]。
- **異常検知:** ネットワークトラフィック、ユーザー行動、システムログなどを常時監視し、通常とは異なる振る舞い（アノマリー）を検知して、潜在的な侵害の兆候を早期に発見する[17]。
- **高度なマルウェア検出:** 既知のシグネチャに頼らず、マルウェアの挙動やコードの特徴を学習し、未知のマルウェアや亜種を検出する[79]。
- **脆弱性管理とリスク評価:** 膨大な脆弱性情報の中から、自組織の環境にとって真に危険な脆弱性をAIが特定し、対策の優先順位付けを支援する[17]。
- **予測的脅威インテリジェンス:** 過去の攻撃データやグローバルな脅威情報を分析し、将来発生しうる攻撃を予測し、事前に対策を講じる[108]。

AIは防御において強力な武器となるが、その「二面性」も認識する必要がある。AI技術自体が攻撃対象となり得るため（敵対的攻撃など）、AIモデル自体のセキュリティ確保も重要な課題となる。

5.3 オペレーショナルテクノロジー（OT）および産業制御システム（ICS）の保護

インダストリー5.0ではOT/ICSのセキュリティ確保がこれまで以上に重要になる。IT環境向けのセキュリティ対策をそのままOT環境に適用するだけでは不十分であり、OT固有の要件（安全性、可用性、リアルタイム性）を考慮した専門的なアプローチが必要となる[16]。

主要なOT/ICSセキュリティ対策には以下が含まれる。

- **ネットワークセグメンテーション:** OTネットワークを機能や重要度に応じてゾーンに分割し、ゾーン間の通信を厳格に制御することで、侵害発生時の影響範囲を限定する[46]。
- **セキュアなリモートアクセス:** 保守や監視のためのリモートアクセス経路を保護し、不正アクセスを防止する。多要素認証やVPNなどの利用が推奨される。
- **OTデバイスの脆弱性管理:** OT環境特有のデバイスやプロトコルの脆弱性を特定し、パッチ適用や代替策（仮想パッチングなど）を計画的に実施する[115]。
- **産業用プロトコルに対応した監視と侵入検知:** Modbus, Profinet, DNP3といったOT固有

の通信プロトコルを理解し、異常な通信や不正なコマンドを検知できる専門のIDS/IPSを導入する[46]。

- **OT環境に特化したインシデント対応計画:** OTシステムへの影響（生産停止、安全上のリスク）を最小限に抑えるためのインシデント対応手順を策定し、定期的に訓練を実施する[116]。
- **OT向けゼロトラスト:** OT環境の特性に合わせてゼロトラストの原則を適用し、デバイスやユーザーのアクセスを厳格に管理する[16]。

5.4 サプライチェーンセキュリティの強化

インダストリー5.0におけるサプライチェーンの複雑性と相互依存性は、セキュリティ上の大きな弱点となり得るため、サプライチェーンリスク管理（Supply Chain Risk Management: SCRM）への積極的な取り組みが不可欠である[19]。

具体的な戦略としては、以下が挙げられる。

- **ベンダーリスク評価:** サプライヤー（ハードウェア、ソフトウェア、サービス提供者）のセキュリティ体制を定期的に評価し、リスクレベルに応じて管理策を要求する[14]。契約にセキュリティ要件を明記することも重要である。
- **ソフトウェア部品表（SBOM）の活用:** ソフトウェアを構成するコンポーネントとその依存関係をリスト化したSBOMを利用し、ソフトウェアの透明性を高め、脆弱性管理を効率化する[27]。
- **セキュアなソフトウェア開発ライフサイクル（SSDLC）:** ソフトウェア開発の初期段階からセキュリティを組み込む（セキュリティ・バイ・デザイン）。自社開発だけでなく、サプライヤーにも同様の取り組みを求める。
- **コンポーネントの真正性と完全性の検証:** 調達するハードウェアやソフトウェアが改ざんされていないか、信頼できるソースからのものであるかを確認するプロセスを導入する[117]。
- **NIST等のガイドライン参照:** NIST（米国国立標準技術研究所）などが発行するサプライチェーンセキュリティに関するガイドライン（例：NIST SP 800-161）を参考に、自社のSCRMプロセスを構築・改善する[117]。

5.5 人間中心のセキュリティ（Human-Centric Security）

インダストリー5.0の核心である「人間中心」の理念は、サイバーセキュリティの設計と運用にも適用されるべきである[20]。これは、セキュリティ対策やツールを設計する際に、それを利用する人間（オペレーター、管理者、従業員）の能力、限界、行動様式、そして使いやすさ（ユーザビリティ）を考慮に入れるアプローチである。

人間中心のセキュリティが意味することは、単に使いやすいインターフェースを提供するだけではない。

- **ユーザビリティとアクセシビリティ:** セキュリティツールやプロセスが直感的で理解しやす

く、日常業務の妨げにならないように設計する [20]。
- 状況に応じたトレーニングと意識向上: インダストリー5.0特有の環境（HMC、AIとの対話など）におけるセキュリティリスクと対策について、従業員に具体的で実践的なトレーニングを提供する [20]。
- 人間工学（ヒューマンファクター）の統合: システム設計段階から人間工学の専門家が関与し、ヒューマンエラーを誘発しにくいインターフェースやワークフローを構築する [21]。
- **AI**による支援: AIを活用して、個々のユーザーに合わせたセキュリティアドバイスを提供したり、リスクの高い操作を検知して警告したりするなど、パーソナライズされた支援を行う [81]。

インダストリー5.0における真の人間中心セキュリティは、従来のように人間を単なる「最も弱いリンク」として管理・統制する対象と見なすのではなく、むしろ現場の状況を最もよく理解し、自動化されたシステムが見逃す可能性のある異常を検知できる重要な「セキュリティセンサー」であり、「協働者」として捉える視点の転換を促す。

その理由は、複雑なHMCやOT環境においては、自動化された検知システムだけでは捉えきれない微妙な異常や、予期せぬ状況が発生しうるからである [83]。日常的に機械やプロセスに触れている現場の作業者は、経験に基づいて「何かがおかしい」と感じ取る独自の能力を持っている [21]。この人間の持つ状況認識能力やドメイン知識を、セキュリティ体制に積極的に活かすべきである。

これを実現するには、使いやすいツールや適切なトレーニングを提供すること [21] に加え、従業員が異常を発見した際に、気兼ねなく、かつ迅速に報告できる明確なチャネルと、報告が奨励されるようなポジティブなセキュリティ文化を醸成することが不可欠となる [20]。これにより、人間は単なる潜在的な脆弱性要因から、AIや自動化された防御システムを補完する能動的な防御参加者へと変貌し、セキュリティ体制全体のレジリエンス向上に貢献するのである [79]。

5.6 脅威と対策のマッピング表

インダストリー5.0特有のサイバー脅威と、それに対応する主要な戦略的対策を関連付けることで、セキュリティ投資の優先順位付けを支援する。

インダストリー**5.0**における主要脅威ベクトル	主要な対策**/**戦略
拡大する攻撃対象領域（IT/OT/IoT融合）	ゼロトラストアーキテクチャ [16], OT/ICSセキュリティ強化（特にセグメンテーション） [46], AI駆動型脅威検知 [98]
AI兵器化/敵対的AI攻撃	AI駆動型防御 [97], AIモデル自体のセキュリティ確保

	（堅牢化、監視）, データ品質管理 [79], 人間による検証プロセス [82]
HMC/Cobotの侵害	適応型ゼロトラスト [16], OT/ICSセキュリティ（安全統合含む） [20], 人間中心セキュリティ設計 [21], 物理的セキュリティ [14]
CPS/デジタルツインの操作	データ完全性保護（暗号化、アクセス制御） [12], リアルタイム監視と異常検知 [69], セキュアなIoT基盤 [101]
高度なランサムウェア（OT焦点）	OT/ICSセキュリティ強化 [27], ゼロトラスト（特にマイクロセグメンテーション） [93], 強固なバックアップと復旧計画, インシデント対応訓練 [116]
高度なサプライチェーン攻撃	サプライチェーンリスク管理（SCRM） [19], SBOM活用 [77], ベンダーセキュリティ評価 [14], セキュア開発プラクティス
内部脅威（人間中心の文脈）	人間中心セキュリティ（意識向上、トレーニング） [21], ゼロトラスト（最小権限） [104], 行動分析（UEBA）, アクセスログ監視

このマッピングは、インダストリー5.0環境における具体的なリスクに対し、どの戦略的アプローチが最も効果的かを判断するための一助となる。

6. 人間機械協働（HMC）におけるセキュリティ考察

インダストリー5.0の中核をなす人間と機械の協働（HMC）は、生産性や柔軟性を向上させる一方で、従来の産業環境にはなかった独自のセキュリティリスクをもたらす。特に、物理的な安全性とサイバーセキュリティが密接に絡み合う点が特徴的である。

6.1 人間とロボットが共有する作業空間における固有のリスク

- 物理的安全とサイバーセキュリティの融合リスク: HMC環境では、サイバー攻撃が直接的な物理的危害を引き起こす可能性がある。例えば、協働ロボット（Cobot）が不正な制御を受けて予期せぬ動作をし、隣で作業する人間に衝突したり、危険な物質を不適切に扱ったりするケースが考えられる [14]。逆に、作業空間への物理的な不正アクセスやCobotへの物理的な改ざん（タンパリング）が、サイバー攻撃の足掛かりとなる可能性もある [14]。
- データ漏洩: HMCプロセス中には、機械の稼働データ、生産データ、品質データなど、様々な情報が生成・交換される。これらが傍受されれば、企業の機密情報が漏洩するリ

スクがある[14]。さらに、作業者のパフォーマンスや状態を監視するシステム（例：認知負荷測定[89]）が導入されている場合、個人のプライバシーに関わるデータが漏洩するリスクも生じる。

- 操作・妨害（**Manipulation/Sabotage**）**:** 悪意のある攻撃者（外部のハッカーまたは内部関係者）がCobotの制御システムを乗っ取り、意図的に誤った動作をさせたり、製品を破損させたり、生産ラインを停止させたりすることが考えられる[14]。最悪の場合、人間の作業員を意図的に危険に晒すような操作が行われる可能性も否定できない。
- 認証の課題**:** 動的で変化しやすい共有作業空間において、人間と機械（Cobot、周辺機器）双方のアイデンティティを確実に認証し、適切なアクセス権限を管理することは、技術的に困難な課題である[14]。不正なユーザーやデバイスがシステムに接続し、操作を行うリスクが存在する。

6.2 Cobotおよび統合HMCシステムの保護

これらのリスクに対応するためには、Cobot自体と、それを含むHMCシステム全体に対する多層的なセキュリティ対策が必要となる。

- **Cobot**本体のセキュリティ**:** Cobotの設計段階からセキュリティを組み込む必要がある。具体的には、不正なソフトウェアの実行を防ぐセキュアブート、通信データの暗号化、アクセス制御機能の実装、脆弱性に対する迅速なパッチ提供体制などが求められる[14]。
- **HMC**セルのネットワークセキュリティ**:** Cobotが動作する作業セルやラインを、他のネットワークセグメントから適切に分離（セグメンテーション）し、ファイアウォール等で通信を制御する[14]。HMC特有の通信パターンや異常な動作を検知できる侵入検知システム（IDS）の導入も有効である。
- データフローの保護**:** 人間、Cobot、センサー、制御システム、上位のAIやデジタルツインシステム間で交換されるデータの機密性と完全性を確保するための暗号化やアクセス制御を実装する[14]。
- 物理的セキュリティ**:** Cobotや関連機器への物理的な不正アクセスや改ざんを防ぐための対策も重要である。作業エリアへの入退室管理、監視カメラの設置、機器へのタンパー検出・防止シール（Tamper-evident seals）の利用などが考えられる[14]。

6.3 安全でレジリエントな協働プロトコルの確保

技術的な対策に加え、HMCの運用ルールやプロトコル自体の安全性と回復力を確保することも重要である。

- セキュアな通信規格とプロトコル**:** HMCにおけるデータ交換や制御命令のための通信規格・プロトコルを策定する際には、初期段階からセキュリティ要件と安全要件を考慮に入れる必要がある[14]。
- フェイルセーフ機構**:** サイバーインシデント発生時や通信途絶時にも、システムが安全な状態（例えば、Cobotが停止する、危険な動作を中断するなど）に移行するようなフェイルセーフ設計が不可欠である[72]。

- 説明可能性と信頼: 特にAIがHMCにおける判断や指示に関与する場合、その判断根拠が人間にとって理解可能であること（説明可能性、Explainability）、そしてシステム全体に対する信頼（Trust）を醸成することが、円滑で安全な協働のために重要となる[75]。

HMCを効果的に保護するためには、単に既存のセキュリティ対策を適用するだけでは不十分である。セキュリティの考慮事項を、協働タスクやワークフローそのものの「設計」段階に深く組み込む必要がある。これは、従来のセキュリティ対策がしばしば実装後や運用段階で追加されるのとは対照的である。

HMCでは、人間と機械の複雑な相互作用[5]から直接セキュリティリスク（物理的アクセス、データ交換、制御の共有など[14]）が生じる。標準的なIT/OTセキュリティ制御（複雑なパスワード、ネットワーク隔離など）をそのまま適用すると、HMCに求められる連携、柔軟性、安全性を阻害する可能性がある[16]。したがって、セキュリティ対策は状況に応じて調整され、ワークフロー設計に統合されなければならない[21]。

安全かつ効果的なHMCワークフローを設計するには、タスクの内容、人間の能力と限界[21]、機械の能力、安全要件[72]、そして潜在的なサイバー脅威[14]を総合的に理解する必要がある。これは、プロセスエンジニア、安全専門家、人間工学専門家[21]、そしてサイバーセキュリティ専門家といった、多様な分野の専門家による緊密な連携を、HMCシステムやプロセスの設計ライフサイクルの「初期段階」から要求する。この「セキュリティ・バイ・デザイン」のアプローチへの転換は、HMCを安全に実現するための鍵となる。

7. データプライバシーと倫理的課題への対応

インダストリー5.0は、そのデータ駆動型の性質と人間中心のアプローチから、データプライバシーと倫理に関して新たな、そして複雑な課題を提起する。膨大なデータの生成・活用と、個人の権利保護や公正性の確保との間で、慎重なバランスを取ることが求められる。

7.1 ハイパーコネクテッド環境におけるデータガバナンス

インダストリー5.0環境では、IoTセンサー、機械の稼働ログ、HMCインタラクション、AIによる分析プロセスなどから、かつてない規模と種類のデータが生成される[7]。この「データの洪水」を適切に管理し、保護することは、極めて重要な課題である。

効果的なデータガバナンス体制の構築が不可欠であり、これには以下の要素が含まれる。

- データの特定と分類: どのようなデータが、どこで、どのように生成・収集・処理・保存されているかを正確に把握（データマッピング）し、その機密性や重要度に応じて分類する[119]。
- 明確なポリシー: データの所有権、アクセス権限、利用目的、保存期間、廃棄方法などに関する明確なポリシーを策定し、組織全体で遵守する[22]。
- アクセス制御: データ分類に基づき、役割や職務に応じてアクセス権限を厳格に管理し、不正アクセスや権限乱用を防止する[118]。

- データ品質管理: データの正確性、完全性、一貫性を維持するためのプロセスを確立する [22]。

7.2 インダストリー5.0のデータフローにおけるGDPRコンプライアンス

EU一般データ保護規則（GDPR）は、個人データの処理に関する厳格なルールを定めており、インダストリー5.0においても重要な法的枠組みとなる [22]。米国のCCPA（カリフォルニア州消費者プライバシー法）/CPRA（カリフォルニア州プライバシー権法）なども関連する規制として挙げられる [23]。

GDPRの主要原則には、適法性・公正性・透明性、目的限定、データ最小化、正確性、保存期間制限、完全性・機密性（セキュリティ）、そして説明責任（アカウンタビリティ）がある [22]。

インダストリー5.0に関連するGDPRコンプライアンス上の課題としては、以下のような点が挙げられる。

- 個人データの特定: 労働者のウェアラブルデバイスからの生体情報、HMI操作ログ、AIによるパフォーマンス分析データ、顧客の個別化注文データなど、インダストリー5.0環境で処理される可能性のある多様な個人データを特定し、GDPRの適用対象となるかを判断する必要がある [22]。
- 同意の取得: 複雑なデータフローの中で、データ主体（労働者や顧客）から適法かつ有効な同意をどのように取得し、管理するかが課題となる [23]。
- データ主体権利への対応: データ主体からのアクセス、訂正、削除（「忘れられる権利」）、処理制限、データポータビリティといった権利要求に、迅速かつ適切に対応できる体制を整備する必要がある [23]。特に、相互接続されたシステムや長期保存されるデータから特定の個人データを完全に削除することは技術的に困難な場合がある [23]。
- データ保護・バイ・デザイン/デフォルト: システムやプロセスを設計する初期段階から、データ保護の原則を組み込むことが求められる [122]。
- 越境データ移転: グローバルなサプライチェーンやクラウド利用に伴う、EU域外への個人データの移転に関する厳格な規則を遵守する必要がある [23]。
- データ侵害通知: 個人データの侵害が発生した場合、規制当局やデータ主体に対して定められた期間内に通知する義務がある [122]。

GDPRは、単なる法的義務に留まらず、組織に対して「適切な技術的および組織的対策」を通じて個人データを保護することを要求しており、堅牢なサイバーセキュリティ体制の構築と密接に関連している [118]。

7.3 産業用AIにおける倫理的懸念への対応

AIはインダストリー5.0の強力な推進力であるが、その利用には倫理的な配慮が不可欠である。

- バイアスと公平性: AIアルゴリズムは、学習に使用されたデータに含まれる偏見を学習・

増幅し、結果として特定のグループに対して不公平または差別的な判断を下す可能性がある[23]。例えば、予知保全アルゴリズムが特定の種類の設備を不当に優先したり、人事関連のAIが特定の属性を持つ候補者を不利に扱ったりするリスクがある。

- 透明性と説明可能性（**XAI**）: 多くの高度なAIモデル（特にディープラーニング）は「ブラックボックス」であり、なぜ特定の結論に至ったのかを人間が理解することが困難な場合がある[75]。特に、安全性や品質に関わる重要な判断をAIが行う場合、その判断根拠の透明性と説明可能性が、信頼と責任の観点から極めて重要になる。
- 説明責任（**Accountability**）: AIシステムが誤った判断を下したり、損害を引き起こしたりした場合に、誰がどのように責任を負うのかという問題。責任の所在を明確にするための枠組みが必要となる[23]。
- プライバシー: AI、特に機械学習モデルは、効果を発揮するために大量のデータを必要とする。このデータの収集・利用プロセスにおいて、個人のプライバシーが侵害されるリスクが常に存在する[23]。匿名化、仮名化、合成データ生成といったプライバシー保護技術の活用が求められる[82]。
- 雇用への影響: AIや自動化技術が人間の仕事を奪うのではないかという懸念は根強い。インダストリー5.0は人間を置き換えるのではなく能力を増強することを目指しているが[43]、スキルの変化に対応できない労働者が取り残されるリスクは依然として存在する。

EUのAI法（AI Act）のような、AIのリスクに基づいた規制アプローチも登場しており、企業はこれらの動向を注視する必要がある[4]。

7.4 イノベーションとプライバシー保護のバランス

インダストリー5.0が目指すイノベーション、効率化、パーソナライゼーションは、データ活用によって大きく推進される。しかし、その一方で、個人のプライバシー権や倫理的配慮をどのように確保するかが大きな課題となる[23]。

技術革新の恩恵を最大限に享受しつつ、個人の権利と尊厳を守るためには、法規制の遵守に加えて、企業自身による倫理的な枠組みの構築、責任あるデータ利活用慣行の確立、そして社会との継続的な対話を通じて信頼を醸成していくことが不可欠である[9]。

インダストリー5.0の「人間中心」という柱は、この点で固有の倫理的緊張関係を生み出す。労働者の幸福や安全を向上させるという目的[4]のために導入される技術、例えば健康状態をモニタリングするウェアラブルデバイス[5]、個々の作業者に合わせてタスクを調整するAI、HMC環境での認知負荷を測定するシステム[89]などは、必然的に労働者に関する機密性の高い個人データを大量に生成する。

これらのデータは、安全確保や作業効率化といった有益な目的のために利用されるとしても、その収集と利用は、監視の強化、労働者の自律性の侵害、あるいはデータに基づいた不公平な評価といった深刻な倫理的懸念を引き起こす可能性がある[23]。GDPRなどの既存のデータ保護法規は重要な基盤を提供するが[22]、インダストリー5.0の人間中心技術によって収集され

るデータの種類と量は、従来の顧客データなどと比較して、はるかに個人的で継続的なものとなり得る。

したがって、単に法規制を遵守するだけでは、人間中心という名の下に収集される労働者データの倫理的リスクに十分に対応できない可能性がある。企業は、インダストリー5.0システムにおける労働者データの収集・利用に関する透明性の高いポリシーと、GDPRを超えるレベルでの厳格なプライバシー保護措置、そして倫理的なガイドラインを積極的に策定・導入する必要がある。これを怠れば、「人間中心」という理念が、結果的に労働者への監視強化を正当化する口実となり、本来目指すべき信頼と幸福を損なうことになりかねない。

8. 戦略的展望と組織への提言

インダストリー5.0への移行は、産業界に大きな変革をもたらすと同時に、サイバーセキュリティに対する新たなアプローチを要求する。将来の脅威動向を見据え、組織は包括的かつ戦略的なセキュリティロードマップを策定し、実行していく必要がある。

8.1 インダストリー5.0を形作る将来のサイバーセキュリティトレンド

GartnerやForresterといった主要な調査会社のリポートは、今後数年間のサイバーセキュリティの方向性を示唆しており、インダストリー5.0の文脈においても重要な示唆を与える。

- **AIの二重の役割:** AIは、攻撃者にとってより巧妙な攻撃（生成AIによるフィッシング、ディープフェイク、適応型マルウェアなど）を可能にする脅威ベクトルであると同時に、防御側にとっても不可欠なツール（AI-SecOps、予測的防御、異常検知）となる [26]。AI対AIの攻防が激化する。
- **サイバーレジリエンスへの注力:** 侵害を完全に防ぐことは不可能であるという前提（"When, not If"）に立ち、侵害発生後の検知、対応、そして迅速な復旧能力（レジリエンス）を重視するアプローチへのシフトが加速する [16]。これはインダストリー5.0の「回復力」の柱と直接的に連携する。
- **攻撃対象領域管理の拡大:** クラウド、IoT、OT、そして人間以外のアイデンティティ（マシンアイデンティティ）を含む、拡大し続けるデジタルエコシステム全体に対する可視性と制御の向上が求められる [26]。
- **技術の最適化と統合:** 単に新しいセキュリティツールを導入し続けるのではなく、既存の投資の効果を最大化し、ツール間の連携を改善することに焦点が移る [26]。
- **セキュリティ文化と人材のウェルビーイング:** 技術だけでなく、従業員のセキュリティ意識と行動を変革するプログラム（SBCP）の重要性が増す。同時に、サイバーセキュリティ担当者の燃え尽き症候群（バーンアウト）を防ぎ、持続可能なチームを維持することも重要な課題となる [26]。
- **サードパーティ/サプライチェーンリスク:** ベンダーやソフトウェアサプライチェーンに起因するリスク管理は、引き続き最優先事項の一つとなる [26]。
- **規制圧力の増大:** プライバシー（GDPR等）、AI（EU AI法等）、サイバーセキュリティ（NIS2

指令、CIRCIA、SEC規則等）に関する各国の規制強化が、セキュリティ投資と実践を後押しする要因となる [16]。

市場予測によれば、インダストリー5.0関連市場および関連するサイバーセキュリティ市場は、今後高い成長率を示すと予想されている [59]。

8.2 包括的なインダストリー5.0サイバーセキュリティロードマップの策定

インダストリー5.0時代のセキュリティ課題に対応するためには、従来のITセキュリティ、OTセキュリティ、HMCセキュリティ、データプライバシー、サプライチェーンセキュリティといった個別の領域を統合した、包括的（ホリスティック）な戦略とロードマップが必要となる [16]。

この戦略策定においては、経営層（取締役会レベル）の積極的な関与が不可欠である。サイバーセキュリティを単なるコストや技術的問題としてではなく、インダストリー5.0の目標（特にレジリエンスと信頼）を達成するためのビジネスイネーブラーとして位置づける必要がある [27]。

既存のセキュリティフレームワーク、例えばNIST Cybersecurity Framework 2.0 [128]、ENISAのガイドライン [91]、産業制御システム向けのIEC 62443 [64]、情報セキュリティマネジメントのISO 27001 [64] などは、ロードマップ策定の基礎として有効である。しかし、これらのフレームワークをそのまま適用するのではなく、インダストリー5.0特有の課題（HMC、AI、IT/OT融合など）に合わせてカスタマイズし、適応させていく必要がある。

8.3 主要な提言

インダストリー5.0への移行を成功させ、その恩恵を安全に享受するために、組織は以下の領域に重点的に取り組むべきである。

- 技術導入:
  - ゼロトラストアーキテクチャの導入を最優先事項とする。
  - AI駆動型の脅威検知・対応ソリューションへの投資を拡大する。
  - OT/ICS環境に特化した堅牢なセキュリティ対策を実装する。
  - リスク評価やシミュレーションのためにデジタルツイン技術を活用する。
  - HMC環境の安全性とセキュリティを両立させる技術（セキュアなCobot、直感的なHMIなど）を導入する。
- 人材育成（ワークフォース・アップスキリング）:
  - セキュリティチームに対して、IT、OT、物理的安全、人間工学（ヒューマンファクター）といった分野を横断する複合的なスキルセットの習得を支援する [21]。
  - 一般従業員に対して、インダストリー5.0環境（HMC、AIとの協働など）に特化したセキュリティ意識向上トレーニングと、機械と安全に協働するためのスキル教育に重点的に投資する [4]。深刻化するスキルギャップへの対応は急務である [26]。
- プロセス適応:
  - すべてのインダストリー5.0関連プロジェクト（HMCシステム設計、AIモデル開発、シス

テム統合など）において、セキュリティとプライバシーを初期設計段階から組み込む（セキュリティ・バイ・デザイン、プライバシー・バイ・デザイン）。
    - IT/OT融合環境に対応したインシデント対応計画を策定し、定期的な訓練を通じて実効性を高める。
    - サプライヤー評価、契約管理、継続的な監視を含む、堅牢なサプライチェーンリスク管理（SCRM）プロセスを確立・運用する。
- ガバナンス:
    - インダストリー5.0におけるセキュリティ、データプライバシー、AI倫理に関する明確なガバナンス体制と責任分担を確立する[23]。
    - 取締役会による適切な監督を確保し、セキュリティ戦略を事業目標と整合させる。
    - IT、OT、安全、エンジニアリング、法務、人事など、部門横断的な連携と協力を促進する文化を醸成する[16]。

8.4 結論：安全で人間中心の産業の未来に向けて

インダストリー5.0は、産業界に効率性や生産性の向上だけでなく、人間性の尊重、持続可能性、そして変化への適応力といった新たな価値をもたらす変革の可能性を秘めている。しかし、その実現は、サイバーセキュリティ、データプライバシー、そして倫理という課題にいかに効果的に対処できるかにかかっている。

インダストリー5.0への移行を成功させるためには、組織はサイバーセキュリティに対して、受動的・部分的な対策から、能動的・包括的、そして人間中心のアプローチへと転換する必要がある。これは、従来のパラダイムからの大きな脱却を意味する。

最終的に、インダストリー5.0の成功は、その核心要素である「人間」「テクノロジー」「持続可能でレジリエントなプロセス」が、相互に「信頼」できる形で統合されるかどうかにかかっている。サイバーセキュリティの確保は技術とHMCへの信頼を、データプライバシーと倫理の遵守は労働者、組織、社会間の信頼を、そしてレジリエンスの実現は産業基盤への信頼を、それぞれ醸成するための基盤となる。

サイバーセキュリティ侵害は技術やHMCへの信頼を損ない[14]、プライバシー侵害や非倫理的なAI利用は個人と組織間の信頼を破壊する[23]。レジリエンスの欠如（サイバー攻撃による機能停止など）は、社会全体の産業への信頼を揺るがす[4]。したがって、サイバーセキュリティ、プライバシー、倫理といった領域を習得することは、単に安全な運用を確保するためだけでなく、インダストリー5.0が約束する価値提案全体を実現するための、根源的かつ戦略的な必須要件なのである。産業、技術、そしてセキュリティは、今後も相互に影響を与えながら、共に進化していくことになるだろう。

引用文献

1. インダストリー5.0とは？製造業での活用方法や現場が抱える課題, 4月 18, 2025にアク

セス、https://www.techs-s.com/media/show/170
2. 「 インダストリー5.0 」船井総研 工場DX.com〜ロボット化自動化、AI・デジタル・Iot、システム化〜, 4月 18, 2025にアクセス、https://smart-factory.funaisoken.co.jp/glossary/240502/
3. research-and-innovation.ec.europa.eu, 4月 18, 2025にアクセス、https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en#:~:text=The%20Industry%205.0%20Award%20provides,centre%20of%20the%20production%20process.
4. Industry 5.0 - European Commission - Research and innovation, 4月 18, 2025にアクセス、https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en
5. 欧州委員会が描く次のデジタル産業革命「Industrie 5.0」を読み解く：第49回 | IT Leaders, 4月 18, 2025にアクセス、https://it.impress.co.jp/articles/-/26221
6. How Do We Define Industry 5.0? - ISG, 4月 18, 2025にアクセス、https://isg-one.com/articles/how-do-we-define-industry-5.0
7. インダストリー4.0からインダストリー5.0への進化 | Mouser Blog ..., 4月 18, 2025にアクセス、https://www.mouser.jp/blog/-the-evolution
8. Industry 5.0 – Smart Factory Glossary - MPDV USA, 4月 18, 2025にアクセス、https://us.mpdv.com/industry-4-0/smart-factory-glossary/industry-50
9. Enabling Technologies for Industry 5.0 | 4BT, 4月 18, 2025にアクセス、https://www.4bt.us/wp-content/uploads/2021/04/INDUSTRY-5.0.pdf
10. インダストリー5.0時代の製造業：人間とロボットの共創 | newji, 4月 18, 2025にアクセス、https://newji.ai/procurement-purchasing/industry5-manufacturing-human-robot-collaboration/
11. Cybersecurity in Industry 5.0: The Most Common Types of Cyber Attacks, 4月 18, 2025にアクセス、https://www.esa-automation.com/en/cybersecurity-in-industry-5-0-the-most-common-types-of-cyber-attacks/
12. A Review on Security and Privacy Issues Pertaining to Cyber-Physical Systems in the Industry 5.0 Era - Tech Science Press, 4月 18, 2025にアクセス、https://www.techscience.com/cmc/v80n3/57887/html
13. Cybersecurity in Industry 5.0: Open Challenges and Future Directions - arXiv, 4月 18, 2025にアクセス、https://arxiv.org/html/2410.09538v1
14. Overcoming Five Cybersecurity Risks of Cobots - Automation.com, 4月 18, 2025にアクセス、https://www.automation.com/en-us/articles/november-2024/overcoming-five-cybersecurity-risks-cobots
15. 2030年のIT基盤へ 積水化学が挑むIT/OTセキュリティの高度化とグローバル標準化 | IT Leaders, 4月 18, 2025にアクセス、https://it.impress.co.jp/articles/-/26879
16. Bridging the gap by integrating zero trust strategies in IT and OT environments for enhanced cybersecurity - Industrial Cyber, 4月 18, 2025にアクセス、https://industrialcyber.co/features/bridging-the-gap-by-integrating-zero-trust-strategies-in-it-and-ot-environments-for-enhanced-cybersecurity/

17. AIが変えるサイバーセキュリティの未来と課題 - Arpable, 4月 18, 2025にアクセス、https://arpable.com/technical-management/information-security/ai-security-technology/
18. パロアルトネットワークス、AIを活用したOTセキュリティの導入を簡素化し61000社を超えるネットワークセキュリティ顧客に提供 - PR TIMES, 4月 18, 2025にアクセス、https://prtimes.jp/main/html/rd/p/000000021.000059751.html
19. 戦略的イノベーション創造プログラム(SIP)第 2 期 IoT 社会に対応したサイバー・フィジカル・セキュリティ「IoT - NEDO, 4月 18, 2025にアクセス、https://www.nedo.go.jp/content/100953484.pdf
20. Systematic Analysis of Risks in Industry 5.0 Architecture - MDPI, 4月 18, 2025にアクセス、https://www.mdpi.com/2076-3417/14/4/1466
21. Safeguarding Critical Infrastructure – Integrating Human Factors in Cyber-Security, 4月 18, 2025にアクセス、https://mimagroup.com/our-thinking/safeguarding-critical-infrastructure-integrating-human-factors-in-cyber-security
22. GDPR 第 5 条: 主要原則と 6 つのコンプライアンスのベスト プラクティス - Exabeam, 4月 18, 2025にアクセス、https://www.exabeam.com/ja/explainers/gdpr-compliance/gdpr-article-5-key-principles-and-6-compliance-best-practices/
23. (PDF) Ethical and Legal Implications of Data in Industry 5.0: Navigating a Hyper-Connected Landscape - ResearchGate, 4月 18, 2025にアクセス、https://www.researchgate.net/publication/389433836_Ethical_and_Legal_Implications_of_Data_in_Industry_50_Navigating_a_Hyper-Connected_Landscape
24. The growing data privacy concerns with AI: What you need to know - DataGuard, 4月 18, 2025にアクセス、https://www.dataguard.com/blog/growing-data-privacy-concerns-ai/
25. Full article: Industry 5.0: a conceptual cybersecurity model for secured digital transformation of enterprises - Taylor & Francis Online, 4月 18, 2025にアクセス、https://www.tandfonline.com/doi/full/10.1080/07366981.2024.2445413?src=
26. Cybersecurity in 2025: The Trends Reshaping Security Strategies, 4月 18, 2025にアクセス、https://nationalcioreview.com/articles-insights/cybersecurity-in-2025-the-trends-reshaping-security-strategies/
27. 5 Key OT Cybersecurity Strategies from the WEF Global Cybersecurity Outlook 2025, 4月 18, 2025にアクセス、https://industrialcyber.co/news/5-key-ot-cybersecurity-strategies-from-the-wef-global-cybersecurity-outlook-2025/
28. インダストリー5.0とは？製造業が目指す未来と取り組むべき課題 | Koto Online, 4月 18, 2025にアクセス、https://www.cct-inc.co.jp/koto-online/archives/431
29. 第5次産業革命（インダストリー5.0）とは？日本の製造業・Society 5.0との関係を考察, 4月 18, 2025にアクセス、https://www.nikken-totalsourcing.jp/business/tsunagu/column/1881/
30. EU Clusters Talks: Industry 5.0: People at the heart of business, 4月 18, 2025にアクセス、https://www.clustercollaboration.eu/content/eu-clusters-talks-industry-50-peopl

e-heart-business
31. Industry 5.0: Towards more sustainable, resilient and human-centric industry - European Commission - Research and innovation, 4月 18, 2025にアクセス、https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/industry-50-towards-more-sustainable-resilient-and-human-centric-industry-2021-01-07_en
32. eurocid.mne.gov.pt, 4月 18, 2025にアクセス、https://eurocid.mne.gov.pt/sites/default/files/repository/paragraph/documents/17991/brochura-industry-50_0.pdf
33. The EU unveils its new Industry 5.0 strategy for social good - 311 Institute, 4月 18, 2025にアクセス、https://www.311institute.com/the-eu-unveils-its-new-industry-5-0-strategy-for-social-good/
34. インダストリー5.0（第五次産業革命）とは？日本・海外における取り組みやテクノロジーの具体例, 4月 18, 2025にアクセス、https://staff.persol-xtech.co.jp/hatalabo/mono_engineer/679.html
35. Industry 5.0 - A Transformative Vision for Europe, 4月 18, 2025にアクセス、https://www.interregeurope.eu/policy-learning-platform/news/industry-50-a-transformative-vision-for-europe
36. インダストリー5.0とは？「次世代の自動化製造」に取り組むメリットや課題、各国の取り組みや歴史的背景を解説 - エムタメ, 4月 18, 2025にアクセス、https://mtame.jp/column/industry_5/
37. インダストリー5.0とは？これまでの産業革命や海外の取り組みも解説 - クラウド実践チャンネル, 4月 18, 2025にアクセス、https://www.cloud-for-all.com/dx/blog/what-is-industry
38. インダストリー5.0が目指す姿 | コンサルタントコラム | 株式会社テクノ経営総合研究所, 4月 18, 2025にアクセス、https://www.tmng.co.jp/column/35873/
39. Industry 5.0 Award - Research and innovation - European Union, 4月 18, 2025にアクセス、https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50/award_en
40. 第五次産業革命：インダストリー5.0とは何か、未来への影響とは？ - SREホールディングス, 4月 18, 2025にアクセス、https://ac.sre-group.co.jp/blog/fifth-industrial-revolution
41. Human-Digital Twins: Enabling Technologies, Applications, and in the Era of Industry 5.0 - BiblioMed, 4月 18, 2025にアクセス、https://www.bibliomed.org/fulltextpdf.php?mno=202670
42. From Industry 4.0 to Industry 5.0: The Transition to Human Centricity and Collaborative Hybrid Intelligence - ResearchGate, 4月 18, 2025にアクセス、https://www.researchgate.net/publication/374701652_From_Industry_40_to_Industry_50_The_Transition_to_Human_Centricity_and_Collaborative_Hybrid_Intelligence
43. Industry 5.0 Technology: Humans and Machines Synergy - Proaction International, 4月 18, 2025にアクセス、https://blog.proactioninternational.com/en/industry-50-technology-human-mach

ine-synergy
44. Industry 5.0: Adding the human edge to industry 4.0 | SAP insights, 4月 18, 2025にアクセス、https://www.sap.com/sea/insights/industry-5-0.html
45. Systematic Analysis of Risks in Industry 5.0 Architecture - ResearchGate, 4月 18, 2025にアクセス、https://www.researchgate.net/publication/378173861_Systematic_Analysis_of_Risks_in_Industry_50_Architecture
46. The role of cybersecurity in Industry 5.0 - Stormshield, 4月 18, 2025にアクセス、https://www.stormshield.com/news/industry-5-0-where-does-cybersecurity-fit-in/
47. インダストリー5.0の基礎知識を解説！製造業が目指すべき未来とは, 4月 18, 2025にアクセス、https://ichengsi.co.jp/ifs-labo/what-industry5/
48. Industry 5.0 vs. Industry 4.0: Main differences and benefits - Inspenet, 4月 18, 2025にアクセス、https://inspenet.com/en/articulo/industry-5-0-vs-industry-4-0-benefits/
49. Industry 5.0: The Role of Collaborative Robots (Cobots) in the New Era, 4月 18, 2025にアクセス、https://www.grandviewresearch.com/blog/role-collaborative-robots-cobots-new-era
50. Industry 5.0: Key differences and can you get a head-start? - Markem-Imaje, 4月 18, 2025にアクセス、https://www.markem-imaje.com/blog/post/from-industry-4.0-to-industry-5.0--what-will-be-the-key-differences-and-how-can-you-get-a-head-start
51. Industry 5.0 vs. Industry 4.0 - Mecalux, 4月 18, 2025にアクセス、https://www.mecalux.com/blog/industry-4-0-vs-industry-5-0
52. 人と技術の融合を深化する「第5次産業革命」とは - Murata Manufacturing, 4月 18, 2025にアクセス、https://article.murata.com/ja-jp/article/what-is-the-fifth-industrial-revolution
53. Top Cybersecurity Trends and Strategies for Securing the Future | Gartner, 4月 18, 2025にアクセス、https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends
54. Industry 5.0 vs Industry 4.0: What are the differences? - ATOSS, 4月 18, 2025にアクセス、https://www.atoss.com/en/insights/blog/from-industry-4-0-to-industry-5-0
55. What is the difference b/w industry 4.0 & industry 5.0? - ResearchGate, 4月 18, 2025にアクセス、https://www.researchgate.net/post/What_is_the_difference_b_w_industry_40_industry_50
56. What are the differences between Industry 4.0 and Industry 5.0? - IndustriALL, 4月 18, 2025にアクセス、https://industriall.ai/blog/what-are-the-differences-between-industry-4-0-and-industry-5-0
57. Differences between Industry 4.0 and Industry 5.0 - Innovapptive Inc, 4月 18, 2025にアクセス、https://www.innovapptive.com/blog/differences-between-industry-4.0-and-indu

stry-5.0
58. Unveiling the Differences Between Industry 4.0 and Industry 5.0 - Lineview Solutions, 4月 18, 2025にアクセス、https://lineview.com/en/unveiling-the-differences-between-industry-4-0-and-industry-5-0/
59. Industry 4.0 vs 5.0: What's the Difference? - Rutgers University, 4月 18, 2025にアクセス、https://engineeringmastersonline.rutgers.edu/articles/industry-4-0-vs-5-0-whats-the-difference/
60. インダストリー5.0市場| 市場規模 市場動向 予測 2024 - 2032年 - グローバルインフォメーション, 4月 18, 2025にアクセス、https://www.gii.co.jp/report/gmi1499344-industry-market-by-technology-by-organization-size.html
61. Digital Transformation 101: What is Industry 5.0? - Innopharma Education, 4月 18, 2025にアクセス、https://www.innopharmaeducation.com/blog/what-is-industry-5-0
62. Most highly cited journal papers with 'Industry 5.0' in their title (February 2023)., 4月 18, 2025にアクセス、https://www.researchgate.net/figure/Most-highly-cited-journal-papers-with-Industry-50-in-their-title-February-2023_tbl2_369305246
63. Industry 5.0: A Survey on Enabling Technologies and Potential Applications - OuluREPO, 4月 18, 2025にアクセス、https://oulurepo.oulu.fi/bitstream/handle/10024/43795/nbnfi-fe202301112375.pdf?sequence=1
64. Cybersecurity for Industry 5.0: trends and gaps - Frontiers, 4月 18, 2025にアクセス、https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1434436/full
65. Industry 5.0: What is it and how does it differ from Industry 4.0? - - Telefónica, 4月 18, 2025にアクセス、https://www.telefonica.com/en/communication-room/blog/industry-5-differences-industry-4/
66. What Is Industry 5.0? - Accu, 4月 18, 2025にアクセス、https://accu-components.com/us/p/459-what-is-industry-5-0
67. The Role of Collaborative Robots in Industry 5.0 - A3 Association for Advancing Automation, 4月 18, 2025にアクセス、https://www.automate.org/robotics/blogs/the-role-of-collaborative-robots-in-industry-5-0
68. インダストリー4.0とは？世界各国の動向と日本の現状をわかりやすく解説！ - 現場改善ラボ, 4月 18, 2025にアクセス、https://www.tebiki.jp/genba/useful/industry4.0
69. Digital Twins in Industry 5.0 – a systematic literatura review, 4月 18, 2025にアクセス、https://epsir.net/index.php/epsir/article/download/641/267/4314
70. Towards a Human-Centric Digital Twin for Human–Machine Collaboration: A Review on Enabling Technologies and Methods - PMC, 4月 18, 2025にアクセス、https://pmc.ncbi.nlm.nih.gov/articles/PMC11013982/

71. インダストリー 5.0：インダストリー 4.0 へのヒューマンエッジの拡大 | SAP のインサイト, 4月 18, 2025にアクセス、https://www.sap.com/japan/insights/industry-5-0.html
72. Cobots: the collaborative heart of Industry 5.0 - From Blog - Fandis SpA, 4月 18, 2025にアクセス、https://blog.fandis.com/en/sci-fa-en/cobots-the-collaborative-heart-of-industry-5-0/
73. What is Industry 5.0? Human-Centricity, Personalization, and Sustainability, 4月 18, 2025にアクセス、https://lineview.com/en/what-is-industry-5-0-human-centricity-personalization-and-sustainability/
74. インダストリー5.0では、優れたAIは人間と同じように思考するようになる - Micron Technology, 4月 18, 2025にアクセス、https://jp.micron.com/about/blog/company/insights/in-industry-5-0-great-minds-will-literally-think-alike
75. Special Issue: Human–Robot Collaboration in Industry 5.0 - ASME Digital Collection, 4月 18, 2025にアクセス、https://asmedigitalcollection.asme.org/computingengineering/article/25/5/050301/1213609/Special-Issue-Human-Robot-Collaboration-in
76. Human-Robot Collaboration | Bench Talk - Mouser Electronics, 4月 18, 2025にアクセス、https://www.mouser.com/blog/eit-2024-human-robot-collaboration
77. Feature Article: Leveraging AI to Enhance the Nation's Cybersecurity | Homeland Security, 4月 18, 2025にアクセス、https://www.dhs.gov/group/13025/news/2024/10/17/feature-article-leveraging-ai-enhance-nations-cybersecurity
78. Role of AI in Cybersecurity: Benefits of AI on Security - EC-Council University, 4月 18, 2025にアクセス、https://www.eccu.edu/blog/the-role-of-ai-in-cyber-security/
79. AI in Cybersecurity: Use Cases, Challenges, and Best Practices - Cynet, 4月 18, 2025にアクセス、https://www.cynet.com/cybersecurity/ai-in-cybersecurity-use-cases-challenges-and-best-practices/
80. AI cybersecurity solutions for enterprise | Verimatrix XTD, 4月 18, 2025にアクセス、https://www.verimatrix.com/cybersecurity/human-and-machine/
81. Human Centric Security Team – Cybersecurity and Quantum Systems - CSIRO Research, 4月 18, 2025にアクセス、https://research.csiro.au/cybersecurity-quantum-systems/about/human-centric-security/
82. AI and Human Collaboration: A Stronger Cybersecurity Defense - Beacon Venture Capital, 4月 18, 2025にアクセス、https://www.beaconvc.fund/research/ai-and-human-collaboration-a-stronger-cybersecurity-defense
83. XAI Human-Machine collaboration applied to network security - Frontiers, 4月 18, 2025にアクセス、https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2024.1321238/full
84. 日本が推し進めるソサエティ5.0とは？インダストリー4.0との違いはあるのか？ | ハルヨ

ン, 4月 18, 2025にアクセス、https://hal4.jp/ks/%E6%97%A5%E6%9C%AC%E3%81%8C%E6%8E%A8%E3%81%97%E9%80%B2%E3%82%81%E3%82%8B%E3%82%BD%E3%82%B5%E3%82%A8%E3%83%86%E3%82%A35-0%E3%81%A8%E3%81%AF%EF%BC%9F%E3%82%A4%E3%83%B3%E3%83%80%E3%82%B9%E3%83%88/
85. インダストリー4.0とソサエティ5.0の違いとは？ | ソニーの開発者ポータル - Sony, 4月 18, 2025にアクセス、https://developer.sony.com/ja/spresense/ai-column/iot-columns/difference-between-industry-4-0-and-society-5-0
86. スマートファクトリーにおける サイバーセキュリティ確保に向けた調査 報告書 - 経済産業省, 4月 18, 2025にアクセス、https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/pdf/001_s02_00.pdf
87. 米国Industry 5.0市場価値は2029年までに651億ドル | e.x.press, 4月 18, 2025にアクセス、https://ex-press.jp/lfwj/lfwj-news/lfwj-biz-market/68770/
88. Security Segmentation in a Small Manufacturing Environment - NIST Technical Series Publications, 4月 18, 2025にアクセス、https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.28.pdf
89. Industry 5.0:Robots reduce workers' cognitive load - cobots - Tobii, 4月 18, 2025にアクセス、https://www.tobii.com/resource-center/scientific-publications/robots-reducing-workers-cognitive-load
90. Industry 5.0 Market Size & Share _ Industry Report, 2030 | PDF | Artificial Intelligence, 4月 18, 2025にアクセス、https://www.scribd.com/document/839613633/Industry-5-0-Market-Size-Share-Industry-Report-2030
91. IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030 - ENISA, 4月 18, 2025にアクセス、https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf
92. Towards a Human-Centric Digital Twin for Human–Machine Collaboration: A Review on Enabling Technologies and Methods - MDPI, 4月 18, 2025にアクセス、https://www.mdpi.com/1424-8220/24/7/2232/review_report
93. タイムテーブル - Security Online Day 2024 秋の陣（2024.09.25-26）, 4月 18, 2025にアクセス、https://event.shoeisha.jp/soday/20240925/timetable
94. 欧州 ENISA 脅威状況 (2023.01-2024.06)：金融セクター, 4月 18, 2025にアクセス、http://maruyama-mitsuhiko.cocolog-nifty.com/security/2025/02/post-ffa151.html
95. Cybersecurity for Industry 4.0 in the current literature: A reference framework | Request PDF, 4月 18, 2025にアクセス、https://www.researchgate.net/publication/328027426_Cybersecurity_for_Industry_40_in_the_current_literature_A_reference_framework
96. Forrester's Top Threats For 2025, 4月 18, 2025にアクセス、https://www.forrester.com/blogs/forresters-top-threats-for-2025/
97. ITmedia Security Week 2024 夏 侵入前提時代、「自社にとっての対策高度化」に欠かせない 構成要素とロードマップ |, 4月 18, 2025にアクセス、

https://members05.live.itmedia.co.jp/library/NzMxMjQ%253D
98. Enhancing Cybersecurity: AI Innovation in Security - Gartner, 4月 18, 2025にアクセス、https://www.gartner.com/en/cybersecurity/topics/cybersecurity-and-ai
99. Cyber Threats | ENISA - European Union, 4月 18, 2025にアクセス、https://www.enisa.europa.eu/topics/cyber-threats
100. (PDF) CyberSecurity Essentials for Industry 5.0 - ResearchGate, 4月 18, 2025にアクセス、https://www.researchgate.net/publication/371230002_CyberSecurity_Essentials_for_Industry_50
101. サプライチェーン・サイバーセキュリティ等に関する 海外の動き - 経済産業省, 4月 18, 2025にアクセス、https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/004_03_04.pdf
102. ENISA AIのサイバーセキュリティと標準化, 4月 18, 2025にアクセス、http://maruyama-mitsuhiko.cocolog-nifty.com/security/2023/05/post-e81218.html
103. Cybersecurity preparedness: What guidance to follow? - Technology Law Dispatch, 4月 18, 2025にアクセス、https://www.technologylawdispatch.com/2024/02/regulatory/cybersecurity-preparedness-what-guidance-to-follow/
104. Implementing Zero Trust Security in the Public Sector - Gartner, 4月 18, 2025にアクセス、https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust
105. STARNET-NEWS Vol.57 - ニュース - スターネット, 4月 18, 2025にアクセス、https://www.starnet.ad.jp/news/starnet-news/vol57/
106. Palo Alto Networks: Leader in Cybersecurity Protection & Software for the Modern Enterprises, 4月 18, 2025にアクセス、https://www.paloaltonetworks.com/
107. Best Network Detection and Response Reviews 2025 | Gartner Peer Insights, 4月 18, 2025にアクセス、https://www.gartner.com/reviews/market/network-detection-and-response
108. The New Era of Cybersecurity: Gartner's Vision for Preemptive Defense - Security Boulevard, 4月 18, 2025にアクセス、https://securityboulevard.com/2024/10/the-new-era-of-cybersecurity-gartners-vision-for-preemptive-defense/
109. ジュニパーネットワークス 製品カタログ, 4月 18, 2025にアクセス、https://www.juniper-ne.jp/common/file/2021ProductGuide_val18.pdf
110. ITトレンド記事コラム | 東芝ITサービス株式会社, 4月 18, 2025にアクセス、https://www.it-serve.co.jp/solution/it_trand/index.htm
111. BlackBerry プレスリリース, 4月 18, 2025にアクセス、https://www.blackberry.com/us/en/regions/ja/newsroom/press-releases
112. 業界最高水準の検証結果とレビュー | クラウドストライク - CrowdStrike.com, 4月 18, 2025にアクセス、https://www.crowdstrike.com/ja-jp/why-crowdstrike/crowdstrike-industry-validation/
113. Software Strategies Blog - Researching the intersection of AI, machine

learning and cybersecurity in the enterprise, 4月 18, 2025にアクセス、https://softwarestrategiesblog.com/
114. Gartner Archives - Software Strategies Blog, 4月 18, 2025にアクセス、https://softwarestrategiesblog.com/tag/gartner/
115. サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）, 4月 18, 2025にアクセス、https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf
116. ENISA「スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス」- IPA, 4月 18, 2025にアクセス、https://www.ipa.go.jp/security/iot/ug65p900000197zo-att/000073490.pdf
117. 経済産業省のサイバーセキュリティ政策について - デジタル庁, 4月 18, 2025にアクセス、https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/9f54b1fb-1a9f-4531-85cb-7659f0458a9b/c22fd9a6/20230911_meeting_technology_based_regulatory_reform_outline_04.pdf
118. Industry News 2024 The Evolving World of Data Privacy Trends and Strategies - ISACA, 4月 18, 2025にアクセス、https://www.isaca.org/resources/news-and-trends/industry-news/2024/the-evolving-world-of-data-privacy-trends-and-strategies
119. Explore the Link Between Cybersecurity and GDPR Compliance | Mandatly, 4月 18, 2025にアクセス、https://mandatly.com/gdpr-compliance/exploring-the-link-between-cybersecurity-and-gdpr-compliance
120. Society 5.0の実現に向けた個人データ保護と活用のあり方【概要】, 4月 18, 2025にアクセス、https://www.keidanren.or.jp/policy/2019/083_gaiyo.pdf
121. GDPR's impact on cybersecurity: A review focusing on USA and European practices, 4月 18, 2025にアクセス、https://ijsra.net/sites/default/files/IJSRA-2024-0220.pdf
122. Navigating Compliance: GDPR and Beyond in Cybersecurity, 4月 18, 2025にアクセス、https://globalcybersecuritynetwork.com/blog/navigating-compliance-gdpr-and-beyond-in-cybersecurity/
123. 最近の欧州デジタル政策 - ベルギー日本人会, 4月 18, 2025にアクセス、http://www.nihonjinkai.be/file/jetro/seminar2017_1_shiryo1.pdf
124. 個人情報保護・プライバシー 2023年の振り返りと2024年の展望 ～欧州編～ | 著書/論文, 4月 18, 2025にアクセス、https://www.noandt.com/publications/publication20240208-2/
125. EU一般データ保護規則（GDPR）への対応支援 | PwC Japanグループ, 4月 18, 2025にアクセス、https://www.pwc.com/jp/ja/services/digital-trust/privacy/gdpr.html
126. AI時代のサイバーセキュリティとは？リスクを最小限に抑えAI価値を最大限に活用する方法, 4月 18, 2025にアクセス、https://www.gartner.co.jp/ja/topics/cybersecurity-and-ai
127. Gartner®: Top Trends in Cybersecurity for 2025 - BitSight Technologies, 4月 18, 2025にアクセス、https://www.bitsight.com/resources/gartner-top-trends-cybersecurity-2025

128. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile - NIST Technical Series Publications, 4月 18, 2025にアクセス、 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf
129. IoT 時代における ICT 産業の構造分析と ICT による 経済成長への多面的貢献の検証に関する調査研究 報告書 - 総務省, 4月 18, 2025にアクセス、 https://www.soumu.go.jp/johotsusintokei/linkdata/h28_01_houkoku.pdf