6.2. IoT を巡る「特許戦争」の可能性

6.2.1. 「特許戦争」を引き起こす要因

■ スマホ特許戦争は「IoT 特許戦争」の先陣？

「モノのインターネット： 産業界のもうひとつの特許戦争？」というタイトルの記事が欧州の知財関係者の間で注目を集めている[5]。この記事の著者は、知的財産権分野で著名な米系法律事務所FinneganのKenie Ho 弁理士。2009 年以降、スマートフォンの特許を巡り、アップル、サムスン、グーグル、HTC、マイクロソフト、ノキアなど多数の企業を巻き込む、世界規模の訴訟合戦が続いていたが、すでに終わりの段階にある。しかし、同記事では IoT を巡り、もっと大規模な「特許戦争」が起こる可能性があると指摘する。スマートフォンは人と人を結ぶだけであったが、IoT は全てのモノを結ぶため、インパクトも巨大になるという。

> **モノのインターネット：もうひとつの産業界の特許戦争？**
>
> **スマートフォンの特許戦争は終わった？IoT の特許戦争が長生きする！**
>
> スマートフォンはパーソナルな IoT 機器の一陣に過ぎない。それと同様に、
>
> 「スマホ特許戦争」はもっと広範囲になると思われる「IoT 特許戦争」の先陣に過ぎない。
>
> （知的財産に特化した米法律事務所 Finnegan の Kenie Ho 弁理士）

■ 「特許戦争」を引き起こす駆動力

同記事で Kenie Ho 弁理士はスマートフォンの特許戦争を引き起こした原因を分析し、なぜ IoT を巡りもっと大規模な特許戦争が起こり得るか分析している。

- **【莫大な経済的影響】**スマートフォンは巨大な市場で、企業にとって訴訟を起こしてでも、自社の特許ポートフォリオを市場シェア獲得のための武器として使う価値があった。IoT 市場はスマートフォン市場の 10 倍の規模になるといわれる。IoT はスマートフォンよりも影響を及ぼす範囲（業界・分野）もはるかに大きい。
- **【多数のテクノロジーの集合体】**スマートフォンは多数の革新的な技術をサブコンポーネントに統合することにより、製品として成り立っている。各サブコンポーネントには、千を超える有効な特許が含まれている可能性がある。このため、特許のクリアランス調査や FTO（Freedom To Operate）分析を完全に行うことが非常に難しく、どのスマートフォンにも特許侵害訴訟のリスクがある。IoT はスマートフォン以上に多くの様々な技術を統合して、システムを構築する必要があり、

[5] 「モノのインターネット： もうひとつの産業界の特許戦争？」の記事は、ブリュッセルで 2016 年 3 月 16 日に開催された、欧州共同体商標協会のワークショップにおける Andreas Thielmann 弁理士（独 COHAUSZ & FLORACK 特許事務所）の発表でも引用されている。

特許侵害訴訟のリスクもより高くなる。

- **【多数の競合企業】**スマートフォンのメーカーは市場シェア競争で接戦を繰り広げてきた。アップル、グーグル、マイクロソフト、ブラックベリーが競合する OS を提供し、同じ OS を採用しているメーカーの間でも市場競争が続く。IoT 市場も同様に、古参の企業や新規に参入した企業が多数、スタートダッシュをかけている。IoT には情報通信以外にも(機械、自動車など)多くの業界が関係し、幅広い活用分野が期待されるため、IoT を手掛ける企業の数はスマートフォンの企業よりも多くなる。プレイヤーが増えれば、法的紛争も生じやすくなる。
- **【多数の規格】**スマートフォンのメーカーは製品に数多くの規格を取り入れる必要があるが、これにより、標準必須特許(SEP)に基づく特許訴訟のターゲットとされる可能性がある。IoT 分野では、すでに数多くの規格が存在し、新たな規格も開発されている。様々な組織が IoT の標準化に向けて活動しており、スマートフォンの特許戦争のときのように、多数の競合する規格が現れてきている。これが IoT の特許戦争の火種となり得る。
- **【大きな特許ポートフォリオ】**通常、それなりの特許ポートフォリオを持っていれば、競合企業からの特許侵害訴訟をかわすことができる。互いに提訴し合うと、費用ばかりがかさみ何の成果も得られない訴訟合戦に陥ってしまうからである。しかし、2009 年にスマートフォン市場が爆発的に拡大し始めると、数社のスマートフォン・メーカーが自社の特許ポートフォリオを武器として、互いに訴え始めた。それが飛び火して業界全体を巻き込み、数えきれないほどの訴訟に発展。IoT に関する特許の出願件数が世界的に大きく伸びており、ある特定の 1 社が大半の特許を抱え込んでいるという状況でもない。スマートフォン企業のように、IoT 企業も防御的な大きな特許ポートフォリオを構築しており、同じ軌道をたどっている。

6.2.2. IoT の特許訴訟の潜在的リスク

■ 標準必須特許(SEP)によるリスク

2016 年 11 月に開催されたドイツ電気技術者協会(VDE)の会議にて、「標準必須特許(SEP) - インダストリー4.0 におけるリスク分析」と題した発表があった。発表者の Joachim Gerstein 弁理士は、インダストリー4.0 や IoT における標準必須特許(SEP)に起因するリスクを指摘。インダストリー4.0 や IoT は、数多くの規格・基準・デファクトスタンダード(業界標準)の利用を前提とする。これらの技術は標準必須特許(SEP)によって保護されており、権利者にライセンス料を支払わなくてはならない。IoT には多数の技術が含まれ、様々な組織が標準化に向けた活動をしていることもあり、標準必須特許(SEP)を全て見つけ出し、それぞれの権利者とライセンスを結ぶことは容易ではない。

■ 幅広い業界の企業が巻き込まれるリスク

Joachim Gerstein 弁理士は、通信業界などこれまでの経験からすると、起こり得る大掛かりな法的紛争にインダストリー4.0 や IoT のサプライチェーン全体が影響を被るとみている。まず最初に攻撃の対象となるのがサプライチェーンの川下の企業だが、**損害賠償請求をサプライヤーに肩代わりさせようとするため、**

オートメーション部品メーカーや電子部品メーカーにも影響が及ぶことになる。

そのような責任の転換が実際に可能かどうかは、基本的にサプライヤーとの契約書の責任条項による。同弁理士は、サプライチェーンの全ての企業が防衛手段を講じる必要があると指摘する。ネットワークで結ばれた生産システムの最終ユーザーにとって、製品に組み込まれている様々な技術のライセンス状況は分かりにくい。サプライヤーが必要な標準必須特許（SEP）のライセンスを持っていることを確かめ、これを契約書に明記し、責任の所在をはっきりとさせる必要があるという。

スマートフォンの特許戦争では、訴訟リスクはIT業界が中心だったが、インダストリー4.0時代には**モノづくりとITの融合が進むため、自動車メーカーや機械メーカーなどリスクにさらされる業種の幅も広がる**。IoTは幅広い分野に影響を及ぼし、他の業界の企業と提携したり、競合したりするため、思いもよらない異業種の企業から攻撃を受ける可能性もある。また、自ら特許を利用して製品をつくるわけではないパテント保有会社・パテントトロールの標的となることもあり得る。このような企業は多数の特許を保有し、事業会社を相手に賠償金や和解金狙いで訴訟を仕掛けてくる。米ソフトウェア大手のマイクロソフトは2017年2月、自社のクラウドコンピューティング・サービスAzureの顧客をパテントトロールから守るために、「Azure IP Advantage」というプログラムを発表した。**特許訴訟から顧客を守るために、自社が保有する特許1万件を顧客が無償で利用できるようにする**という。

■ 国境を越える訴訟のリスク

国境を越えてネットワークで結ばれた生産システムでは、**国内での行為により、第3国での特許侵害に加担してしまう潜在的リスク**があるとJoachim Gerstein弁理士は指摘する。ネットワーク化された生産システムでは、国内から生産プロセスを制御し第3国で生産ステップの一部を実行することも可能なため、結果として第3国における特許侵害となってしまう危険がともなう。

独オートメーション部品メーカーifm electronicのDr. Hans Kornmeier氏は、ネットワークで結ばれたデジタルの世界では特許侵害の場所を突き止めることが次第に難しくなると指摘する。同氏は2016年7月、「知的財産権デー」にて「知的財産権とインダストリー4.0」というタイトルで講演した。クラウドコンピューティングでは、ビックデータが世界の「どこか」で処理されるが、それが実際にどこかは（ユーザーではなく）そのクラウドサービスを提供している企業が決める。また、ネットワークで結ばれた生産環境では、特許請求（クレーム）の各項が異なる国で使われるかもしれない。例えば、3つの工程段階（a1、a2、a3）のある製法特許をドイツで取得したとし、ドイツでa1、米国でa2、イギリスでa3の工程段階が行われるかもしれない。国境を越えた（クロスボーダー）特許侵害のリスクが高まる。

■ ドイツの裁判所の重要性

無線LANに接続した事務機器監視装置に関する特許を巡り、2014年にサムスンがパテント保有会社Penoviaから提訴されるなど、IoTの特許訴訟の例はすでにあるが、現在のところスマートフォンの特許戦争のようなレベルには至っていない。ドイツの著名特許事務所BOEHMERT & BOEHMERTのChristian W. Appelt弁理士は弊社の取材に対し、「IoTの経済的重要性が高まれば、激化する市場競争の中で特許が武器として使われることは確かである。しかし、必ずしも“特許戦争”になるとは限らず、多くの特許係争はクロスライセンスを交わし合うなど（訴訟を回避して）平和的に解決されるかもしれない。それでも、IoT

分野の特許侵害訴訟が今後、増加するだろう」としている。ドイツの裁判所は「世界の特許裁判所」として知られ、スマートフォンの特許戦争でも中心的な役割を果たした。特にデュッセルドルフの裁判所は専門性が高く、迅速で、他国と比較しても訴訟費用が低く、(権利者の利益となるよう)侵害者にとっては厳しい措置を取ることも厭わない。このため、IoT の特許訴訟でも重要な役割を果たすと思われる。

ドイツにおける「IoT 特許バトル」の可能性について

特許侵害訴訟の専門家 Jens Künzel 弁護士
(KRIEGER MES & GRAF v. der GROEBEN 法律事務所)による見解

中期的には、モノのインターネット(IoT)に関してドイツで「特許バトル」が繰り広げられる可能性が高い。しかし、現時点ではまだその兆候は現れておらず、ドイツにおける IoT 分野の訴訟は知られていない。「特許バトル」がまだ始まっていない理由として、下記の 3 つが考えられる。

1. IoT 分野の特許保護された技術・製品が**まだ大量に使用されていない**。スマートフォンのように市場規模が大きく拡大し、特許を侵害した製品が多く出回ってくると、特許の金銭的な関心も大きくなり、数多くの特許訴訟が起こると思われる。
2. IoT 特許の出願件数はここ数年で急激に増加しており、この分野で出願された特許の多くは**まだ付与(権利化)されていない**。
3. IoT 分野では、**広範囲に及ぶ「技術標準」がまだなく**、標準必須特許(SEP)の侵害訴訟の証拠立てを難しくしている(SEP 訴訟では、その標準が実際に使用されていることが前提条件となる)。

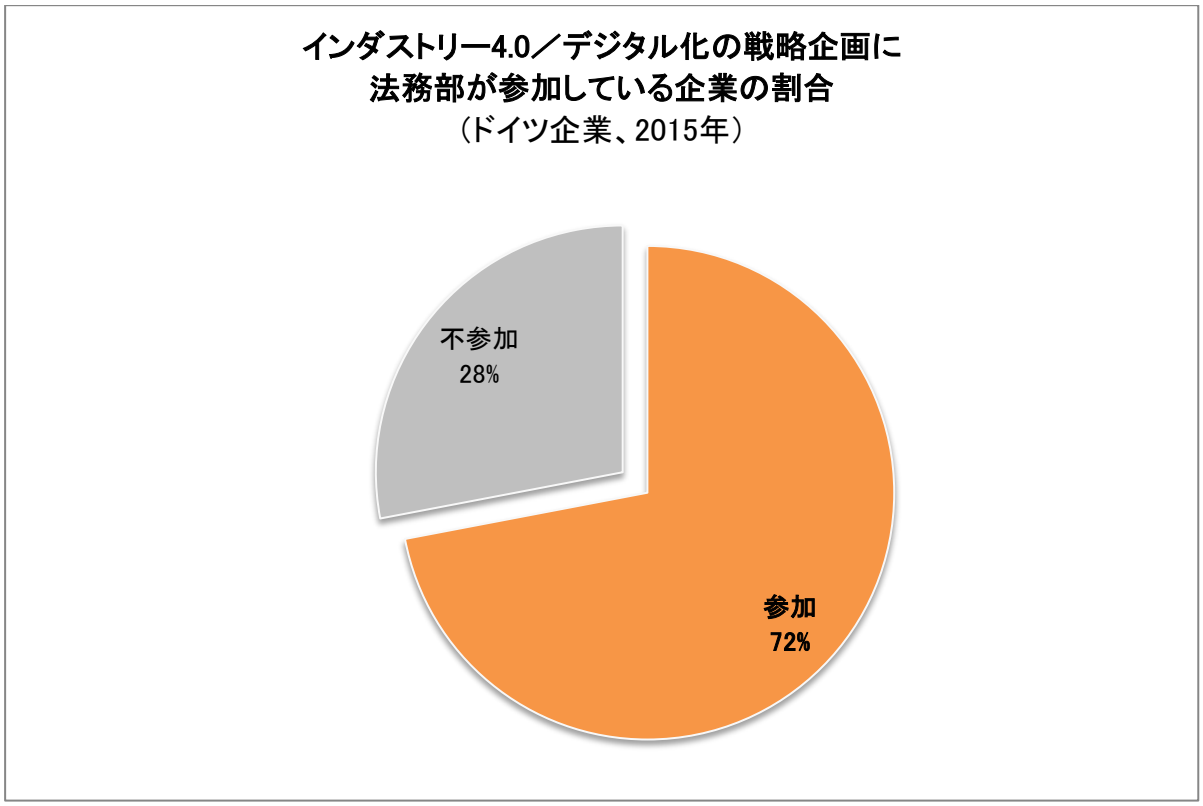
特許侵害訴訟では従来から、欧州レベルで**「シグナル」となる注目される判決を望む、多くの外国企業がドイツを訴訟地として選んでいる**。ドイツ(特にデュッセルドルフ)の裁判官は特許訴訟に豊富な経験を有し、複雑な案件にも適切に対処することで知られているからである。今後、世界的な「IoT 特許戦争」が起こった場合、「スマホ特許戦争」の際と同様にドイツの裁判所がリーダー的な役割を果たすと予想される。それは、欧州統一特許裁判所の新制度の開始後も変わらないとみられている。

6.3. インダストリー4.0／IoT に関する法的問題

■ 7 割の大企業で、法務部がインダストリー4.0 に関与

製造業のデジタル化は法律分野にも様々な課題をもたらす。ドイツ産業連盟（BDI）は「インダストリー4.0 － デジタル化にともなう法的課題」のレポートの中で、「デジタル化戦略の企画やそれに対応した製品・ビジネスモデルの開発の際に、企業は早い段階から法務部に助言を求める必要がある」としている。同レポートによると、ドイツの 7 割の大企業ではインダストリー4.0 の戦略的企画に法務部が参加している。特に、「今後 5 年以内にデジタル化が自社のビジネスモデルに大きな影響をもたらす」と考えている企業では、この割合が大きい。

図 53：インダストリー4.0 の戦略企画に法務部が参加している企業の割合（ドイツ）

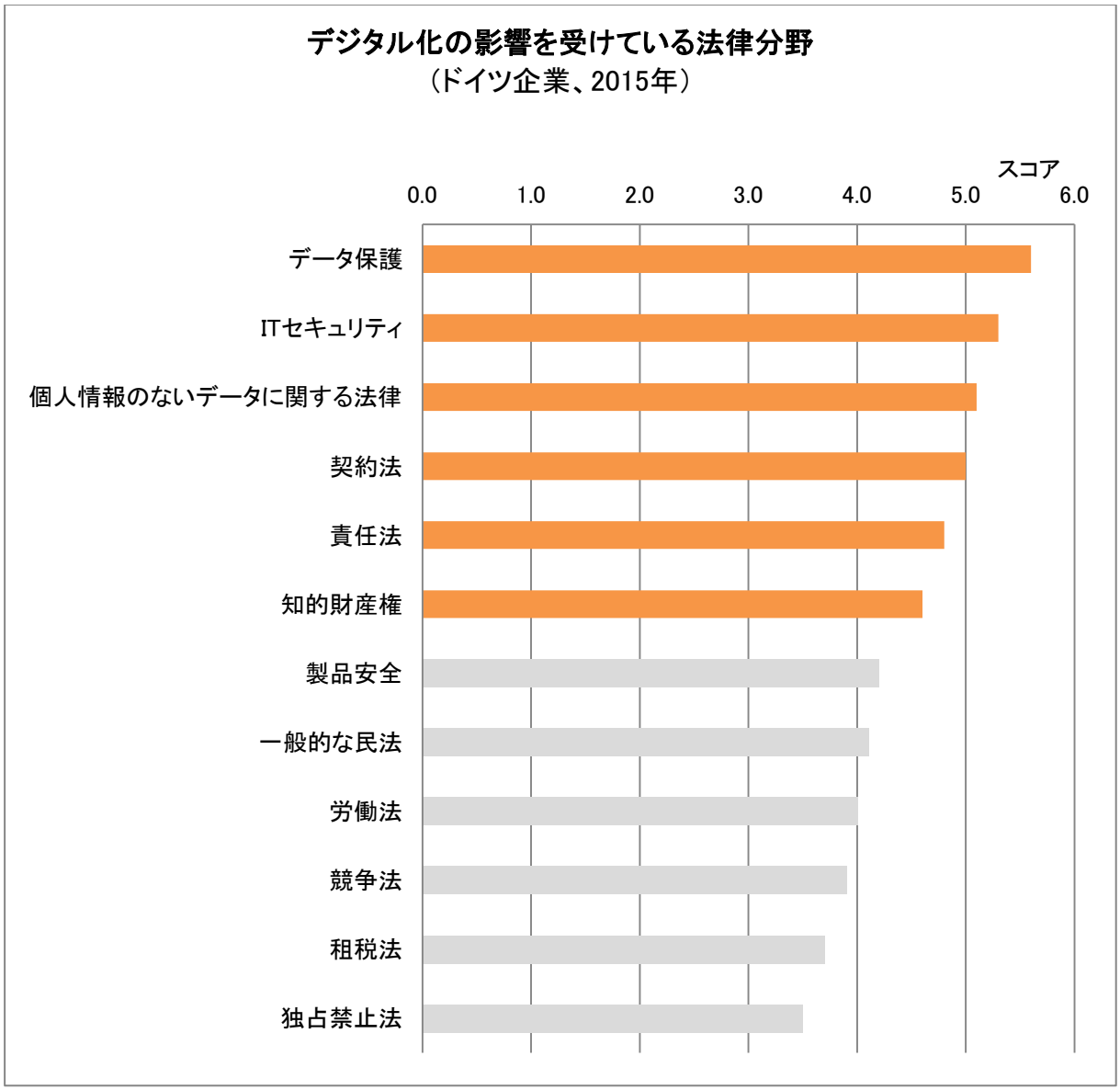


調査対象：ドイツの主要企業（91 社）　　出所：BDI/Noerr

■ データに関する法律がトップテーマ

ドイツ産業連盟（BDI）は同国の主要企業の法務部を対象としたアンケート調査で、「貴社では、デジタル化によりどの法律分野が影響を受けていますか？」と設問。次ページの図に示す回答をみると、「データ保護」、「IT セキュリティ」、「個人情報の含まれない（機械が生成する）データの所有権」といった、データに関する法律が上位を占める。「契約法」、「責任法」、「知的財産権」も重要視しているが、労働法、競争法、独占禁止法は差当り大きな問題ではないとみている。

図 54: デジタル化の影響を受けている法律分野(ドイツ)



調査対象:ドイツの主要企業(91 社)　　出所:BDI/Noerr

【データの所有権】

インダストリー4.0 の世界はデータの世界で、データが物を言う。センサーが収集しサーバーに送られてくる「データは誰のものか」という問題は経済的に非常に重要である。オートメーション技術メーカーifm electronics の Dr. Hans Kornmeier 氏は、「データの所有権がまだ明確に規定されていない」と指摘する[6]。Cohausz & Florack 特許事務所の Andreas Thielmann 弁理士も将来の課題として、データの所有権の問

[6] 独 ifm electronics 社の Dr. Hans Kornmeier 氏は 2016 年 7 月、「産業財産権デー」にて「知的財産権とインダストリー4.0」のテーマで講演し、データの所有権の問題に言及した。

題を挙げている[7]。ドイツ産業連盟（BDI）のレポート「インダストリー4.0 － デジタル化にともなう法的な課題」では、「当面の間はデータの使用権について各企業に任せ、契約書で定めるべき」と結論付けている。このため、機械の購買契約書や保守契約書などで、**データの所有権と使用権（データが誰のもので、データを用いて誰が何をすることが許されるか）について明確に定める必要**がある。

【データ保護】

インダストリー4.0 のサイバーフィジカルシステムでは、サプライチェーン全体がネットワークで繋がれる。サプライヤーや顧客企業と緊密に協力し合うようになり、競合企業とも協業する機会が増えてくる。データの所有権とともに、データ保護やデータセキュリティが新たに重要となる。インダストリー4.0／IoT の大きな活用分野と期待される予知保全でも、データ保護とデータセキュリティの問題は避けて通れない。

ドイツのデータ保護法（BDSG）で定められているのは個人データの保護のみで、純粋な機械データは対象ではない。しかし、（例えばユーザーの特性を分析するために）**従業員や顧客のデータを機械データと組み合わせると、データ保護法の対象となり得る**。Gunnar Helms 弁護士は独専門誌 MaschinenMarkt（機械市場）への寄稿記事で、予知保全・遠隔保守に関して下記の点をアドバイスする。

1. 予知保全・遠隔保守に際して、個人に関するデータを全く収集しない。
2. 上記が回避できない場合は、匿名化するなどして個人情報を取り除く。
3. 個人データも分析したい場合は、該当する個人にはっきりと許可を得るなど、データ保護法に抵触しないよう十分に配慮する。

【データセキュリティ】

データセキュリティは、許可を得ていない第三者によるシステムへの不正アクセス、攻撃、データの悪用から守ることを目的とする。データ、データバス、ネットワークに繋がっている機械やロボット、（スマートフォンやタブレット端末など）IoT 機器の全てがサイバー攻撃の対象となり得る。IoT サービスの多くがスマートフォンやタブレットを介して操作できるようになっているが、スマートフォンやタブレット端末の OS の脆弱性に付け込まれる恐れもある。実際に**産業スパイ、妨害行為、恐喝を目的とした、遠隔保守システムを狙ったサイバー攻撃が発生**しているという。

ドイツのデータ保護法（BDSG）はデータセキュリティに関して 9 条で定めているが、主として個人データをサイバー攻撃や不正アクセスから守ることを目的としている。2015 年に発効した IT 安全法では、IT セキュリティの最低基準や IT セキュリティ事故の通知義務を定めているが、主な適用対象は（エネルギー、医療、金融、通信など）重要インフラの事業者である。**ドイツ情報セキュリティ庁（BSI）は遠隔保守システムが悪用されるリスクが大きいとみており、同庁のホームページ上で遠隔保守システムを守るためのガイダンスを公開**している（https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html）。

[7] Andreas Thielmann 弁理士（Cohausz & Florack 特許事務所）は欧州共同体商標協会（ECTA）のワークショップで「モノのインターネット：特許」のタイトルで講演し、その中でデータの所有権の問題を取り上げた。

【労働安全】

インダストリー4.0／IoT 環境では機械・設備や製品がインターネットに接続されるため、**サイバー攻撃が（火災、感電など）物理的な危険につながり、従業員にも被害が及ぶ恐れ**がある。また、**人間とロボットが協調して働くダイナミックな環境とあり、労働安全に多大な影響**を与える。サイバーフィジカルシステムを不正侵入や誤操作から守ることは大きな課題となる。従来は機械安全を IT セキュリティと切り離して扱っていたが、今後、**セーフティ（労働安全）とセキュリティの相互作用**が生じるようになる。

【法的責任】

インダストリー4.0 では生産システムが自動化され、機械同士がコミュニケーションを取り合う。そのようなシステムでエラーや損害が生じた場合、法的責任の所在が問題となる。人間に起因する場合は現行の責任法を適用することができるが、人間が介入できない自動化されたシステムではどうすべきか法的課題となっている。Lawentus 法律事務所の Gunnar Helms 弁護士は、「**人間が関与することなしに、機械が損害を引き起こした場合の法的責任の所在を契約書で定めることが不可欠**」としている（ただし、ドイツの法律では一般条項で法的責任に関して定められる範囲がかなり制限されている）。

※ 付加製造（3D プリント）

付加製造（3D プリント）技術によって、個々の顧客の要望に合わせた製品（バッチサイズ 1）の生産が可能になる。従来の大量生産では試作品（またはパイロット生産の製品）を検査・認証すれば済んだが、製品の**バッチサイズが 1 となると、企業内の品質管理や外部機関による製品安全試験・認証をどうすべきか新たな課題**にぶつかる。また、付加製造された製品の安全性に誰（3D プリンターのメーカー、原料の納品業者、3D プリンターのユーザーなど）が責任を持つかという法的問題もある。付加製造された製品の品質管理、検査、認証、法的責任に関して現在、空白がある。

【契約法】

インダストリー4.0 で機械同士がコミュニケーションを取り合い、機械が「意思表示」をする場合、そのような「意思表示」を民法上、どのように扱うかという問題がある。例えば、「自己学習」したコンピューター・システムがスペア部品を自動的に再発注した場合、そのような「注文」に法的拘束力があるかという問題である。ドイツの法律では、契約上の意思表示は法的行為能力のある人間が行う原則に基づく。自律システムには基本的に法的行為能力がなく、法的拘束力のある意思表示を行うことはできない。機械同士が人間を介在せずに相互に情報交換し、自動的に最適な制御が行われるシステムでは、機械による「意思表示」が法的な意味合いを持つべきか契約上、明確にする必要がある。CBH 法律事務所の IT 法の専門家 Dr. Sascha Vander 弁護士は、**機械が生成する「意思表示」の法的拘束力について契約書で定める**ことを強く奨励する。

【知的財産権と模倣品】

インダストリー4.0 によるデジタル化やネットワーク化の進展は企業だけではなく、模倣犯罪者にも新たな可能性をもたらす。例えば、**3D プリント技術により（その製品の CAD データを入手すれば）模倣品の作製が容易**になる。このため、3D プリントに必要な CAD データが狙われる。ドイツ機械工業連盟（VDMA）の「模倣品レポート」では、「工場のネットワーク化が進むにつれ、製品、機械、生産設備全体の**企業秘密が**

攻撃にさらされることが多くなる」と指摘する。今後、製品やノウハウの保護がより重要となる。

■ デジタル化した経済 ― アナログの法律？

ドイツ産業連盟（BDI）は 2016 年 2 月、ベルリンとブリュッセルで「インダストリー4.0 デジタル化した経済 ― アナログの法律？」と題した会議を開催し、産学官の代表者と下記の課題について議論した。

- **【データ保護法】**「21 世紀の石油」といわれるデータをどう取り扱うべきか。プライバシー保護とどう折り合いをつけるべきか。
- **【個人情報を含まないデータ】**個人情報を含まない（機械や自動車が生成する）データにはデータ保護法が適用されないが、どう取り扱うべきか。IoT によって、そのようなデータが大量に生成されるが、明確に定めた法規制がない。誰に所有権、使用権、課金する権利があるのか。
- **【製造物責任】**モノがデータを生成するだけではなく、自動的に決定を下して行動した場合、どうなるのか。自動運転の車や自動制御ロボットが損害を起こした場合、誰が責任を負うのか。運転者・操作員か、所有者か、メーカーか、ソフトウェアのサプライヤーか。
- **【刑法】**ソフトウェアが「学習」し、自動的に改善・発展していった場合はどうなるのか。元のプログラマーが責任を負うべきか。民法だけではなく、刑法の観点からはどうか。
- **【著作権法】**ソフトウェアが自動的に「考え」て、絵、音楽、文章を創作した場合、著作権はどうなるのか。

ドイツ産業連盟（BDI）によると、企業側の参加者はデータに関する法的問題に頭を悩ませているという。個人データをどう取り扱ったらよいか、個人とは関係のないデータには何の法律が適用されるのか、データセキュリティの何を満たさなくてはならないのか、といった問題である。

■ インダストリー4.0 にともなう法的問題のコンファレンス「Netlaws」

2017 年 2 月下旬、インダストリー4.0、e ヘルス、スマート・モビリティにともなう法的問題のコンファレンス「Netlaws」がニュルンベルクで開催された。誰がデータを所有するのか、誰が責任を負うのかといった問題は法的状況が明らかではなく、企業に不安をもたらし、インダストリー4.0 普及の妨げとなっている。Netlaws は技術者と法律家の橋渡しをして、その対処法を探るのが目的で、ドイツやスイスから 150 人以上の参加者が 2 日間、デジタル化やネットワーク化にともなう法的問題ついて議論した。**大概のケースでドイツの法律は充分で、当面は新しい規則で対応すれば事足りる**という結論に達したという。また、「法的コンプライアンス」の観点から、今後、**法律家がもっと製品開発に参加すべき**という。基調講演は米 Google 社のドイツ現地法人の法務責任者 Dr. Arnd Haller 氏が行った。同氏はデジタルトランスフォーメーションは法律家にとっても大きな課題とし、Google 社にも全ての答えがあるわけではなく、デジタル化の法的課題は徐々に克服されていくだろうとした。次回の「Netlaws」コンファレンスは 2018 年 2 月に開催予定。バイエルン州経済省が後援し、ヴュルツブルク大学法学部ロボット法研究センターが顧問を務める。

■ インダストリー4.0 のための法律参照モデル

ドイツ経済エネルギー省が助成するテクノロジー・プログラム「Autonomik für Industrie 4.0（インダストリー

4.0 のためオートノミック）」は 2017 年 5 月、インダストリー4.0 のための法律参照モデル「Ju-RAMI 4.0」のオンライン版を作成した（www.ju-rami-online.com）。**法律の素人向けのガイダンスで、インダストリー4.0 の開発から販売までの過程で留意すべき法的状況について、初歩的な情報**が得られる。ドイツ企業が問題状況に気付き、問題解決のために法律専門家と議論する準備ができるよう構成されている。

下記の 7 つのリスク分野をカバーする。

- **人的損害**
- **物的損害**
- **契約違反**
- **個人データの悪用**
- **機械の制御不能**
- **労働者の権利の侵害**
- **知的財産権の侵害**

各リスク分野について、実例を用いて下記の点を詳細に解説している。

- 起こり得るリスク
- リスクを回避するための予防措置
- 判例
- 法律面からのケース分析
- アドバイス
- 考慮すべき法律分野

下記の法律分野が含まれている。

- 民法（法的責任）
- 民法（契約責任）
- 刑法
- データ保護
- 労働安全衛生法
- 知的財産権