ソシオネクストの知財戦略：ソリューションSoCの基盤

エグゼクティブサマリ

本レポートは、株式会社ソシオネクストの知的財産戦略について、公開されている一次情報に基づき、その構造、特徴、およびビジネスモデルとの連関性を網羅的に分析したものです。

- ソシオネクストの知財戦略は、同社独自の「Solution SoC」ビジネスモデルと不可分に統合されています[1]。
- 同社は知的財産を、単なる法的権利ではなく、「他社製品との差別化を図るための技術やノウハウ」そのものと定義し、企業価値の源泉として位置づけています[1]。
- 2015年の設立は、富士通およびパナソニックのLSI事業を継承したものであり[52] [55]、初期の知財ポートフォリオはこの両社の技術資産を基盤に形成されたと推察されます。
- 現在の特許出願戦略は、「2nm以降の先端プロセスノード」および「チップレット技術」という、次世代のSoC開発に不可欠な二大優先分野へ高度に「集中」しています[1]。
- NRE（非経常収益）の海外比率増加に対応し、日本国内出願と並行して「外国出願」を積極的に推進する「グローバル」戦略を採択しています[1]。
- 組織体制の最大の特徴は、知財グループを法務部門ではなく「開発グループ内」に設置している点です[1] [31]。これにより、R&D（研究開発）と知財創出のサイクルが一体化されています。
- ファブレス企業特有の重大リスクである「OSS（オープンソースソフトウェア）の不適切な利用」[1]に対し、専門の「ソフトウェア管理推進グループ」を設置しています[1]。
- さらに、国際標準規格「OpenChain ISO/IEC 5230:2020」認証を取得しています[1]。これは、半導体業界（OSS脆弱性リスクが全業界で最も高いとされる[23]）において、極めて高度なコンプライアンス体制の証左であり、顧客への「信頼」の提供という攻めの戦略にもなっています。
- ファブレスモデル固有のもう一つのリスクである「技術・ノウハウの漏洩」[1] [31]も公式に認識しており、厳格な管理（主に企業秘密としての保護）が実行されていると見られます。
- 競合他社（Broadcom[9]、Marvell[13]、Renesas[39]）とは異なる戦略を採用しています。特に、多くのハイテク企業（Google、Tesla、主要自動車メーカー全社[48] [49]）が加盟するPAE（特許トロール）防衛網「LOT Network」に、本調査時点で加盟していない[5]（[6]の調査結果）点が顕著な特徴です。
- この非加盟という戦略的スタンスは、PAEからの訴訟リスクを将来的に抱える一方で、特許ポートフォリオ活用の自由度を確保する意図がある可能性が示唆されます。

背景と基本方針

設立の経緯と初期ポートフォリオの形成

株式会社ソシオネクスト（以下、ソシオネクスト）は、2015年3月2日に事業を開始しました[53]。同社は、富士通株式会社（以下、富士通）およびパナソニック株式会社（以下、パナソニック、現パナソニックホールディングス株式会社）のシステムLSI事業を統合し、株式会社日本政策投資銀行（DBJ）からの出資を受けて設立された、いわゆる「カーブアウト（事業分離）」案件です[52] [54] [55]。設立時の出資比率は富士通40%、パナソニック20%、DBJ 40%であり[54] [55]、日本の大手エレクトロニクス企業二社が数十年にわたり蓄積してきた強力な技術基盤、人材、そして広範な知的財産ポートフォリオを継承してスタートした点に、同社の知財戦略の原点があります。

この「カーブアウト」という出自は、同社の知財戦略を分析する上で極めて重要です。同社はゼロからスタートしたのではなく、富士通とパナソニックが保有していた膨大な、しかし設立時点（2015年）では一部レガシー化していた可能性もある特許群を、初期資産として保有していたと推察されます。したがって、同社の設立以来の知財戦略は、単なる新規出願の積み増しではなく、「初期の継承ポートフォリオをいかに整理・活用し、"新生ソシオネクスト"独自のビジネスモデルに合致した、未来志向の新規ポートフォリオを構築し直してきたか」という点に本質があると分析されます。この初期資産の存在が、後述する最先端分野への「集中」戦略を可能にした土台であるとも考えられます。

CSR基本方針と知財の定義

ソシオネクストは、そのCSR基本方針において、知的財産を「企業価値の源泉」と明確に定義し、その保護と尊重をうたっています[1]。注目すべきは、同社が知的財産を単なる特許権や商標権といった法的な権利（Legal Rights）としてのみ捉えているのではなく、「他社製品との差別化を図るための様々な技術やノウハウ」そのものとして、より広範な経営資産（Business Assets）として認識している点です[1]。

この定義は、同社のビジネスモデルと深く関連しています。半導体業界において「IP（Intellectual Property）」という用語は、二重の意味を持っています。一つは、本レポートの主題である特許権や著作権などの法的な「知的財産権」です。もう一つは、特にLSI（大規模集積回路）の設計開発において用いられる、特定の機能を実現するためのモジュール化された回路設計データ、いわゆる「IPコア」です[2] [3]。

ソシオネクストの知財戦略は、この両方の「IP」を巧みに連動させています。同社は、R&D活動を通じて後者の「IPコア」（＝技術・ノウハウ）を創出し、それを顧客の要求に応じて組み合わせ、最適化することで「Solution SoC」というカスタム製品（ASIC）として提供します。そして、そのビジネスの優位性を守るために、前者である法的な「知的財産権」（特許や企業秘密）を行使します。同社の知財戦略

は、このビジネスモデルの根幹を成す「技術・ノウハウ」の保護・活用そのものであると言えます。

「Solution SoC」ビジネスを支える知財活動

ソシオネクストは、知財活動の明確な目的を「『Solution SoC』モデルに基づいた事業の優位性を強化すること」と設定しています[1]。この「Solution SoC」モデルは、汎用品（ASSP）の大量生産・販売ではなく、特定の顧客が抱える固有の課題を解決するために、オーダーメイドの半導体（カスタムSoC）を設計・開発し、その対価としてNRE（Non-Recurring Engineering：非経常収益、開発設計料）を受け取るビジネスです[6]。

このモデルにおいて、知財活動は決定的な役割を果たします。同社は、最先端技術への投資によって生み出された「技術やノウハウ」（＝IPコア）を、特許や機密情報（トレードシークレット）として適切に保護・管理することによって、事業の優位性を強化するとしています[1]。

この活動の最終的なゴールとして、同社が「顧客からの信頼をさらに獲得する」[1]ことを挙げている点は、特に示唆に富んでいます。カスタムSoCビジネスにおいて、顧客（例えば、大手自動車メーカーやデータセンター事業者）は、自社製品の心臓部であり、競争力の源泉でもある半導体の設計・開発を、ソシオネクストという外部パートナーに委ねるという重大な経営判断を行います。

この判断において、顧客が最も重視する点の一つが「信頼」です。具体的には、①ソシオネクストが提供する技術（IPコア）が、他社の特許を侵害しておらず、将来にわたって訴訟リスク（＝供給停止リスク）がないこと、②ソシオネクストが自社の技術・ノウハウを法的に強固に保護しており、競合他社に模倣されるリスクが低いこと、そして③（第4章で詳述しますが）自社（顧客）の機密情報や設計データが、ソシオネクストのサプライチェーンを通じて漏洩するリスクがないこと、の3点が挙げられます。

ソシオネクストの知財戦略は、単に自社の技術を防衛するという受動的な側面に留まらず、これら顧客の懸念を払拭し、「信頼」を醸成するための、積極的な営業・マーケティングツールとしても機能していると分析されます。

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 2. https://www.socionext.com/en/download/catalog/AD00-00006-2E.pdf
- 3. https://www.socionext.com/en/download/catalog/AD00-00006-1E.pdf
- 6. https://www.socionext.com/jp/download/catalog/AD00-00006-2.pdf

52. https://www.socionext.com/en/ir/pdf/sn_ir20250829_01e.pdf
- 53. https://www.socionext.com/en/pr/sn_pr20150302_01e.pdf
- 54. https://www.fujitsu.com/global/about/resources/news/press-releases/2015/0302-02.html
- 55. https://www.sec.gov/Archives/edgar/data/63271/000119312515243551/d948256d6k.htm

全体像と組織体制

R&Dと一体化したガバナンス

ソシオネクストの知的財産ガバナンス体制における最大、かつ最も戦略的に重要な特徴は、その組織配置にあります。同社は、「知的財産活動を主導する知的財産部門（知財グループ）を、開発部門（開発グループ）の中に設けています」[1] [31]。

この組織設計は、多くの日本企業において知財部門が法務部門や管理部門の配下に置かれ、主に「発明が生まれた後」の出願手続きやライセンス契約、訴訟対応といった「下流（ダウンストリーム）」の業務を担うケースとは、明確に一線を画すものです。

ソシオネクストのこの「R&D埋め込み型（Embedded）」の体制は、同社のビジネスモデルを遂行する上で、極めて合理的な意図を持った組織設計であると推察されます。知財グループがR&D部門（開発グループ）の内部に存在することにより、単なる発明の発掘や出願手続きに留まらず、R&Dの最も「上流（アップストリーム）」である技術戦略の策定段階から、知財の専門家が深く関与することが可能になります。

例えば、新しい技術分野（例：「2nm」や「チップレット」）への研究開発投資を決定する際、開発グループ内の知財グループは、競合他社の特許網（パテントマップ）を即座に分析し、どの領域に「空白地帯（チャンス）」があり、どの領域に「地雷原（リスク）」があるかをR&Dチームにフィードバックすることができます。これにより、他社特許を回避する設計（デザイン・アラウンド）を初期段階から織り込み、R&D投資の無駄を省くとともに、将来的に価値の高い特許（＝Solution SoCの差別化要因）を戦略的に創出することが可能になります。

この体制は、取締役会の監督の下、開発グループ本体、法務グループ、そして知財グループが密接に連携し、サービス・製品の開発段階から知財リスクへの対応までをシームレスに推進する[1]ための

基盤となっています。第1章で述べた「技術・ノウハウ」がそのまま「商品（IPコア）」となり、その保護（特許）がビジネスの優位性に直結する同社にとって、R&Dと知財は分離不可能です。この組織体制は、知財戦略とR&D戦略を完全に一体化して実行するための、最も合理的かつ効率的な形態であると考えられます。

OSSリスクに対応する専門組織

ソシオネクストの知財ガバナンス体制において、R&D埋め込み型の知財グループと並んで注目すべき点が、もう一つの専門組織の存在です。同社は、開発グループ内に、通常の知財グループとは別に、「著作物やオープンソースソフトウェア（OSS）を含むソフトウェアの適切な管理を推進するためのソフトウェア管理推進グループ」を設置しています[1]。

この「知財の二重体制」とも言える組織構造は、極めて示唆に富んでいます。これは、現代のSoC（System-on-Chip）開発における知的財産リスクが、伝統的な「ハードウェア特許」のリスクと、「ソフトウェア（特にOSS）」のリスクという、根本的に性質の異なる2種類のリスクから構成されていることを、同社が明確に認識し、それぞれに専門家を充てている証左です。

SoCは、シリコンチップ（ハードウェア）と、その上で動作する膨大なソフトウェア（ファームウェア、ドライバ、OS、ミドルウェア）が一体となって初めて機能します。このソフトウェア部分において、開発効率や機能性の観点からOSSの利用は不可避であり、その利用機会は増加の一途をたどっています[1]。

しかし、OSSの利用には、ハードウェアの特許侵害とは全く異なる種類の、深刻な知財リスク（ライセンス違反）やセキュリティリスク（脆弱性）が伴います。この詳細については第5章で詳述しますが、このOSS特有のリスクに対応するには、特許法務とは異なる、ソフトウェア工学、ライセンス体系、および脆弱性管理に関する高度な専門知識が要求されます。

したがって、この二重体制は、極めて合理的な専門分化であると分析されます。「知財グループ」は、主に自社で創出する資産（ハードウェア設計、回路、アルゴリズム）の特許や企業秘密による「保護」と「活用」を担当します。一方、「ソフトウェア管理推進グループ」は、主に外部から導入する資産（OSS）のライセンス「遵守（コンプライアンス）」と脆弱性「管理（リスク回避）」という、より防衛的かつプロセス管理的な役割を担っていると推察されます。この専門分化により、それぞれの領域で高度な専門性を発揮できる体制を整えている点は、同社の知財戦略の成熟度の高さを示すものとして高く評価されます。

公式なリスク認識

ソシオネクストは、知的財産リスクマネジメントにおいて、自社のビジネスモデルを取り巻く主要なリス

クとして、以下の3点を明確に公式文書で認識し、対策を講じているとしています[1] [31]。

1. 第三者の権利侵害に起因する訴訟・係争リスク
2. 技術やノウハウの漏洩リスク
3. **OSS（Open Source Software）**の不適切な利用リスク

この3点のリスク認識は、同社の「Solution SoC」ビジネスモデル、および「ファブレス」という業態を的確に反映しています。

(1) は、カスタムSoCという多機能・高集積なチップであるがゆえに、必然的に他社が保有する多数の要素技術（特許）に抵触する可能性が高まるという、半導体業界共通の、しかし極めて深刻なリスクです。
(2) は、自社で工場を持たず、製造を外部のファウンドリやOSATに委託する「ファブレス」モデル特有のリスクです。設計データ（＝技術・ノウハウ）を第三者に開示するプロセスで、その漏洩や盗難が発生するリスクを指します。
(3) は、前述の通り、現代のSoC開発に不可避なソフトウェア・サプライチェーンに内在する、ライセンス違反やセキュリティ脆弱性に関するリスクです。
ソシオネクストの知財戦略は、単に特許を取得するという「攻め」の側面だけでなく、これら3つの重大な経営リスクにいかに体系的に対処するかという「守り」の側面が、その核心部分を形成していると考えられます。

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 31. https://www.socionext.com/jp/download/catalog/AD00-00006-2.pdf

詳細分析①：特許ポートフォリオ戦略（「集中」と「グローバル」）

レガシーから最先端への「集中」

ソシオネクストは、限られたR&Dリソースを知的財産の観点から最大化するため、明確な「選択と集中」戦略を採用しています。同社は、主要なフォーカスエリア（Automotive, Data Center & Network, Smart Devices, Industrial Equipment）向けのカスタムSoC開発において、特に鍵となる技術分野を「優先的な技術分野」として指定し、そこに特許出願リソースを集中投下しています[1]。

具体的に、同社が優先分野として公表しているのは、以下の二分野です[1]。

1. **2nm**（ナノメートル）以降の先端プロセスノードを含む先端技術
2. チップレット技術

この二分野の選定は、同社の将来の技術的・戦略的方向性を明確に示しています。「2nm以降」とは、半導体の回路線幅を指し、ムーアの法則の最先端、すなわち半導体「製造」プロセスの最先端を追求する意志を示しています。一方、「チップレット」とは、従来のように一つの巨大なチップ（モノリシック）に全機能を集積するのではなく、機能ごとに最適化された小さなチップ（チップレット）を個別に製造し、それらを基板上で高性能に接続・統合する、最新の「設計・実装」方法論です。

この二つは、いわば次世代半導体の「車の両輪」であり、ソシオネクストが、単なる既存技術の組み合わせ（インテグレーション）に留まらず、次世代の「Solution SoC」ビジネスの核となる最先端技術の創出そのものにR&Dリソースを集中していることを示しています。

Google Patentsなどのデータベースで確認される同社の既存の特許資産（例：画像処理装置[20]、ホームゲートウェイ装置[22]、イコライザ回路[21]など）には、第1章で述べた富士通・パナソニック時代からの「レガシー資産」が広範に含まれている可能性が高いと見られます。これに対し、現在の知財戦略は、これらレガシー資産の防衛・維持にリソースを割くのではなく、明確に次世代のビジネスに不可欠な最先端技術にリソースを振り向け、質の高い特許ポートフォリオを構築するという、「未来志向」の「集中」戦略であると分析されます。

NRE収益に連動した「グローバル」出願

ソシオネクストの特許出願戦略のもう一つの柱は、その「グローバル」な展開です。同社は「NRE（非経常収益）収益における海外市場の割合増加を考慮し、国内（日本）出願に加え、外国出願も積極的に推進しています」[1]と明記しています。

これは、同社の「Solution SoC」ビジネスモデルと特許戦略がいかに密接に連動しているかを示す、非常に重要な記述です。前述の通り、「Solution SoC」ビジネスでは、特定の顧客（例：米国のデータセンター事業者、欧州の自動車メーカー）との共同開発契約（NRE）が収益の柱となります。

このビジネスフローにおいて、NRE契約が成立し、共同開発が始まる段階で、その成果として発明（技術・ノウハウ）が生まれます。この発明（特許）は、その技術が最終的に使用される市場、すなわち「顧客の市場」で保護されていなければ、ビジネス上の意味を持ちません。

したがって、NRE収益の海外比率の増加は、そのまま外国出願（特に顧客の主要市場である米国、欧州、中国など）の必要性の増加に直結します。同社の知財部門（知財グループ）が、R&D部門（開発グループ）の内部に存在する[1]という利点を活かし、ビジネス部門とも緊密に連携しながら、NRE契約の受注見込みや収益が期待される国・地域を戦略的に特定し、出願リソースを効率的に配分する（＝儲かる場所で特許を取る）という、極めて合理的でROI（投資対効果）の高いグローバル出願戦略を実行していると推察されます。

ポートフォリオの定量的側面（推定）

ソシオネクストの有価証券報告書（2025年8月29日発行版）[52]の目次には「II 事業の状況 6. 研究開発活動」のセクションが存在することが示されています（ただし、[9]のスニペット分析によれば、具体的な保有特許件数などの詳細は本文ページ（P.48）に含まれるため、公開スニペットからは確認できません）。

参考として、半導体業界の競合他社の例を挙げると、Marvell Technology（マーベル・テクノロジー）は、2019年時点で10,000件以上の特許を保有している[13]と公表しています。

ソシオネクストは、富士通・パナソニックからのカーブアウトという経緯（第1章参照）を踏まえると、設立当初から一定規模の継承ポートフォリオを保有していることは間違いありません。しかし、前述の「集中」戦略の分析から、同社がMarvellのような「量（Portfolio Volume）」を追う戦略を採っているとは考えにくいです。

同社の戦略は、保有件数（Stock）の多さを競うのではなく、R&D戦略と連動した「2nm/チップレット」[1]という最先端分野において、NRE収益（＝ビジネス）[1]に直結する「グローバル」な主要市場（米、欧、中など）で、競合の参入障壁となり得る質の高い「未来の」特許（Flow）を、選択的かつ集中的に確保することにあると分析されます。

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 13. https://www.marvell.com/company/newsroom/marvell-named-a-derwent-top-global-innovator-for-the-seventh-consecutive-year.html
- 20. https://patents.google.com/patent/US8738860B1/en
- 21. https://patents.google.com/patent/EP2101455A2/zh
- 22. https://portal.unifiedpatents.com/patents/patent/US-10530839-B2
- 52. https://www.socionext.com/en/ir/pdf/sn_ir20250829_01e.pdf

詳細分析②：ファブレス・エコシステムとハードウェアIP防衛

ファブレスモデル固有のリスク構造

ソシオネクストは、自社で半導体製造工場（ファブ）を持たない「ファブレス」企業です[18]。巨額の設備投資（数千億円規模とも言われる[18]）が必要な製造プロセスを外部に委託し、自社は「Solution SoC」の設計・開発という上流工程（知的資産の創出）に特化することで、高い資本効率とビジネスのスピードを実現しています。

製造は、TSMC（台湾）やSamsung（韓国）に代表される「ファウンドリ」（半導体受託製造企業）や、ASE（台湾）などに代表される「OSAT（Outsourced Semiconductor Assembly and Testing）」（後工程の組立・検査受託企業）[3]といった、グローバルな半導体エコシステム（サプライチェーン）のパートナーに委託されます。

このファブレスモデルは、設備投資リスクを回避できる[18]一方で、半導体業界特有の、極めて深刻な知的財産リスクを内包します。それは、自社の競争力の源泉である「設計データ（IP）」、すなわち「技術・ノウハウ」の「漏洩リスク」[1] [31]です。

設計が完了したSoCを製造するためには、その詳細な設計データ（GDSIIファイルなど）を、製造委託先であるファウンドリやOSATといった第三者に開示・移転する必要があります。このグローバル化・多層化したサプライチェーン[17] [33]の中で、設計データ（IP）がひとたび流出すれば、以下のような深刻な被害が生じる可能性があります[17] [33]。

1. 設計**IP**の窃盗とリバースエンジニアリング**:** 競合他社が設計データを不正に入手し、分析・模倣することで、ソシオネクストが巨額のR&D費用を投じて開発した技術が容易に盗まれる。
2. 無断での過剰生産（**Counterfeiting**）**:** 委託先が契約した数量以上にチップを無断で製造し、非正規の市場（グレーマーケット）に安価で流通させる。
3. ハードウェアへの「トロイの木馬」挿入**:** 設計データに、悪意ある第三者によって不要な回路（スパイチップやバックドア）が挿入・改ざんされ、製品のセキュリティや信頼性が根本から損なわれる。

ソシオネクストは、このリスクを「技術やノウハウの漏洩リスク」[1] [31]として、経営上の重要リスク（第2章参照）の一つとして公式に認識しています。これは、同社のビジネスの根幹である「Solution SoC」の設計データ（＝差別化の源泉）が、ファウンドリやOSATとのグローバル・サプライチェーン[17] [33]の中で漏洩・悪用されることへの強い警戒感を示すものです。

ハードウェア**IP**防衛戦略（トレードシークレット）

ソシオネクストは、この深刻な「漏洩リスク」を低減するための措置を講じている[1]としています。

しかしながら、有価証券報告書（[9]の分析結果）やサステナビリティ報告書（[1]）において、次章で述べるOSSコンプライアンスに関する具体的な取り組み（専門組織の設置、ISO認証の取得[1]）と比較して、このハードウェアIPの漏洩防止に関する具体的な技術的・体系的手段（例えば、設計の難読化（Obfuscation）、動的カモフラージュ[33]、ハードウェア・ウォーターマーク（電子透かし）、PUF（Physically Unclonable Function：物理複製不能関数）の利用等）については、公にされていません。

この「非公開性」こそが、ハードウェアIP防衛戦略の核心である可能性が極めて高いと推察されます。

次章で詳述するOSSコンプライアンス戦略は、その「遵守プロセス」を国際標準（ISO）で認証し、それを公表・アピールすること自体が、顧客（特に車載やデータセンター）への「信頼」の証となり、競争優位に繋がります。

一方で、ハードウェアIPの防衛策は、その性質上、「どのような対策を講じているか」という手の内を秘密にすること自体が、最も強力な防衛戦略（＝企業秘密、トレードシークレット）となります。どのような難読化技術を使っているかを公表すれば、それを解読する攻撃手法が開発されてしまうからです。

したがって、ソシオネクストのハードウェアIP防衛は、公表されている以上に厳格な、以下の三層の組み合わせで構成されていると考えられます。

1. 法的防衛（契約）：ファウンドリやOSATとの間で、設計データの取り扱い、機密保持、監査権限、違反時の罰則などを含む、極めて厳格な契約（NDA、製造委託契約）を締結する。
2. 物理的・電子的防衛（管理）：開発プロセスにおける設計データへの厳格なアクセス管理、データ移転時の暗号化、委託先における管理体制の監査・徹底。
3. 技術的防衛（非公開）：前述した「動的カモフラージュ」[33]や設計難読化、ウォーターマークといった、リバースエンジニアリングや改ざんを技術的に困難にする手法を、公表せずに設計データ自体に組み込む。

特に、同社が注力する「2nm/チップレット」[1]という最先端技術（第3章参照）は、世界でも限られた最新鋭のファウンドリ（例：TSMC、Samsungなど）でしか製造が不可能です。これは、取引先（＝漏洩リスク源）がごく少数に限定されることを意味し、結果として、かえって厳格な機密管理と深いパートナーシップの構築が可能になっている側面もあると推察されます。

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 3. https://www.socionext.com/en/download/catalog/AD00-00006-1E.pdf
- 17. https://gigazine.net/news/20181129-dynamic-camouflaging-approach-on-chip/

- 18. https://hasegawa-kakosho.com/faburesukigyou/
- 31. https://www.socionext.com/jp/download/catalog/AD00-00006-2.pdf
- 33. https://gigazine.net/news/20181129-dynamic-camouflaging-approach-on-chip/

詳細分析③：ソフトウェア・サプライチェーンとOSSコンプライアンス戦略

半導体業界における深刻なOSSリスク

現代のSoC（System-on-Chip）は、もはや単なるハードウェア（シリコンチップ）ではなく、その上で動作する複雑なソフトウェア（ファームウェア、ドライバ、OS、ミドルウェア、アプリケーション・ライブラリ）と一体となった「ソリューション」として提供されます。このソフトウェア・スタックの開発において、開発期間の短縮、コスト削減、および高度な機能の実装のために、OSS（オープンソースソフトウェア）の利用は不可避であり、その重要性は増大の一途をたどっています[1]。

しかし、このOSSの利用は、半導体業界にとって「諸刃の剣」となっています。シノプシス（Synopsys）社が2024年4月に発表した「オープンソース・セキュリティ＆リスク分析（OSSRA）」レポート[23]は、この分野における極めて深刻な実態を明らかにしています。

この調査によれば、「コンピュータ・ハードウェアおよび半導体」業界のコードベース（ソフトウェア資産）は、OSSの利用において、調査対象となった全業界の中で最悪レベルのリスクを抱えていることが判明しました[23]。
具体的には、以下の2点において、全業界でワースト1位となっています[23]。

1. 高リスクの**OSS**脆弱性**:** 調査対象のコードベースのうち、実に**88%**（全業界平均は84%）が、高リスク（既知の重大なセキュリティ上の欠陥）のOSS脆弱性を含んでいました。
2. ライセンス競合**:** コードベースのうち、**92%**（全業界平均は53%）が、OSSライセンスの競合（例えば、GPLのようなコピーレフト型ライセンスのOSSを、非公開の商用製品に不適切に組み込んでいる）の問題を含んでいました。

この客観的データは、ソシオネクストが経営上の重要リスクとして「OSSの不適切な利用リスク」[1]を特定（第2章参照）している背景を、強力に裏付けています。

不適切なOSSを利用した場合のリスクは、二重に深刻です。第一に「法的リスク」です。ライセンス違

反（前述の92%が該当する問題）が発覚した場合、ライセンス違反による「知的財産（著作権）侵害訴訟」に発展し、製品の出荷停止、損害賠償、あるいは最悪の場合、自社のSoC（あるいはその上で動くソフトウェア）のソースコードの公開を命じられる可能性があります。第二に「セキュリティリスク」です。高リスクの脆弱性（前述の88%が該当する問題）を放置したままSoCを出荷した場合、ハッカーによる攻撃の標的となり、データの窃盗やシステムの乗っ取りを許すことになります。

特にソシオネクストの注力分野である「Automotive（車載）」（＝人命に関わる）や「Data Center & Network（データセンター）」（＝機密情報や社会インフラに関わる）[1]において、これらのリスクは文字通り「致命的」な問題であり、顧客の信頼を根本から失墜させるものです。

「OpenChain ISO/IEC 5230」認証取得の戦略的意義

この半導体業界全体が抱える深刻なOSSリスク（「業界の不都合な真実」とも言える[23]）に対し、ソシオネクストは極めて具体的、体系的、かつ高度な対策を講じています。

その対策は、二つのステップで構成されています。

第一のステップは、第2章で述べた組織体制の構築です。同社は、開発グループ内に、特許を扱う「知財グループ」とは別に、OSSを含むソフトウェアの適切な管理を専門に推進する「ソフトウェア管理推進グループ」を設置しました[1]。これにより、OSSのリスク管理に必要な高度な専門知識（多様なライセンス体系の理解、脆弱性スキャンツールの運用、ソフトウェア部品表（SBOM）の管理など）を組織的に担保する体制を整えました。

第二のステップは、その体制（プロセス）の客観的な証明です。ソシオネクストは、この「ソフトウェア管理推進グループ」の活動をさらに強化・体系化し、OSSコンプライアンスに関する国際標準規格である「**OpenChain ISO/IEC 5230:2020**」の認証を取得しています[1]。

この「OpenChain ISO/IEC 5230」認証の取得は、同社の知財戦略において、極めて重大な戦略的意義を持っています。これは単なる内部的なリスク管理（守り）に留まるものではありません。OpenChain ISO認証は、ソフトウェア・サプライチェーン全体（SoCベンダー、部品メーカー、最終製品メーカー）で、OSSのコンプライアンス（ライセンス遵守や脆弱性管理）を確実にするための「プロセス（体制）」が、国際標準に準拠していることを、第三者機関が客観的に認めたものです。

ソシオネクストは、この認証取得を、「防衛（リスク回避）」のためだけではなく、顧客に対する「攻め（信頼の獲得）」の戦略的ツールとして活用していると分析されます。

前述の通り、半導体業界のコードベースの92%がライセンス違反のリスクを、88%が脆弱性リスクを抱えている[23]という客観的データがある中で、ソシオネクストは、自社の顧客（特にコンプライアンスに世界で最も厳格な欧州の自動車メーカーや、米国のデータセンター事業者）に対し、「当社のSolution SoCに組み込まれるソフトウェア・スタックは、他社のようなリスクの温床ではなく、国際標準（ISO）のプロセスで適切に管理・検証されており、ライセンス・セキュリティの両面で信頼できる」とい

う、客観的な証拠に基づいた強力なメッセージを発信することが可能になります。

これは、他社に対する明確かつ強力な差別化要因（「Proven Trust」）となり、NRE契約の獲得において、技術的な優位性（2nm/チップレット）と並ぶ、あるいはそれ以上に重要な「信頼」という価値を提供し、ビジネスの優位性を強化するものと高く評価されます。

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 23. https://www.synopsys.com/ja-jp/japan/press-releases/2024-04-17-2.html

競合比較

多様な半導体知財戦略モデル

ソシオネクストの知財戦略（ビジネスモデルとR&Dに融合し、特にOSSコンプライアンスという「信頼」を重視する戦略）の独自性を理解するため、他の主要な半導体企業（ファブレス/IDM）の知財戦略モデルと比較分析します。

- Broadcom（ブロードコム）：
  Broadcomの戦略は、知財を「市場を奪取し、防御するため」の強力なビジネス武器として明確に位置づけている[9]点が特徴です。単にイノベーションを守るだけでなく、高品質な特許ポートフォリオを構築し[7]、必要に応じて他社に対する積極的な特許訴訟（オフェンシブな活用）も辞さない戦略が随所に見られます[10] [11]。例えば、同社が買収したVMWareを、後述する防衛的な特許コミュニティ（LOT Network）から脱退させようとした動き[7]は、特許の活用（ライセンス収益や売却益を含む）の自由度を最大限に確保しようとする、攻撃的な姿勢の表れとも解釈できます。
- Marvell Technology（マーベル・テクノロジー）：
  Marvellの戦略は、R&Dの「イノベーション（革新性）」を知財戦略の中核に据えています。同社は10,000件を超える特許ポートフォリオを保有し[13]、その質の高さ（特許の被引用数など）が評価され、Clarivate社から「Top 100 Global Innovator」に7年連続で選出される[13]など、技術革新と知財の連動を強くアピールしています。ただし、その一方で、過去にはカーネギーメロン大学（CMU）との特許侵害訴訟において、11.7億ドル（最終的には和解）という巨額の賠償判決を受ける[12]など、アカデミアとの侵害リスク管理において大きな課題に直面した歴史も有しています。
- Renesas Electronics（ルネサス エレクトロニクス）：
  IDM（垂直統合型）メーカーであるルネサスは、その知財活動を経営戦略・事業戦略と「融合」させるための、精緻な組織論・方法論を構築・実践している点が特徴的です。例えば、知財部門

が「経営幹部」「他社」「事業部門」をそれぞれ主要顧客と見立てて最適化を図る「トロイカ体制」[39]や、知財活動を単なる出願・権利化に留めず、「創生」「育成」「活用」「対策」「貢献」「開発」という6つのカテゴリーに再定義する[39]など、知財を経営資産として全社的に活用するための体系的な仕組みを重視しています。

最大の分岐点：PAE防衛網「LOT Network」への非加盟

これら競合他社との比較において、ソシオネクストの知財戦略における最大、かつ最も注目すべき戦略的相違点は、PAE（Patent Assertion Entity：特許主張主体、いわゆる「パテント・トロール」）への防衛策にあります。

PAEは、自ら製品を製造・販売することはなく、他社（時には経営難の企業）から買い集めた特許のみを資産として、製品を販売する企業（特にハイテク企業）に対して特許侵害訴訟を提起し、巨額のライセンス料や賠償金を得ることをビジネスモデルとしています。ボストン大学の研究によれば、こうしたPAEによる訴訟は、米国だけでも年間約600億ドルの直接的損害を与えているとされ[49]、ハイテク企業にとって深刻な経営リスクとなっています。

このPAEリスクに対する防衛策として、2014年に設立されたのが、非営利の防衛コミュニティ「**LOT Network**」です[49]。これは、加盟企業（Google, Canon, Red Hatが創設メンバー[49]）が保有する特許が、万が一PAEの手に渡った（売却された）場合、その特許に対する無償のライセンス（行使の免除）が、他の全加盟企業に対して自動的に付与されるという仕組みです。これにより、PAEは加盟企業に対して訴訟を起こす「武器」を失い、コミュニティ全体がPAEのリスクから守られることになります。

このLOT Networkは急速に支持を広げ、2024年8月時点で4,300社以上が加盟し、450万件以上の特許資産がこの防衛網に含まれています[49]。加盟企業には、Google, Microsoft, IBM, Netflix, SAP, Teslaといったハイテク大手に加え[49]、ソシオネクストの主要な顧客層であり、特許訴訟の格好のターゲットでもある「世界の上位**7**社の自動車メーカー」すべてが加盟しています[48] [49]。

本レポートの調査時点において、LOT Networkが公式サイトで公開しているメンバーリスト（[6]が[6]を検索した結果）に、「Socionext」または「ソシオネクスト」という名前は確認されませんでした。

この「非加盟」という事実は、ソシオネクストの知財戦略における、極めて重大な戦略的スタンスを示しています。これは、同社が（加盟料コストや他の理由から）単に加盟していないというレベルに留まらず、意図的にこのグローバルな防衛網の「外」にいることを選択している（あるいは、加盟の必要性を現時点では認めていない）ことを意味します。

この「非加盟」の理由として、いくつかの仮説が立てられます。

1. 戦略的自由度の確保（**Broadcom**型）**:** LOTに加盟すると、自社特許をPAEに売却して高額な利益を得たり、自らPAE的にライセンス交渉を行うといった「オフェンシブ（攻撃的）」な活用が著しく制限されます。BroadcomのVMWare脱退の動き[7]にも見られるように、特許の活用方法（売却

益含む）の自由度を最大限に保持したいという、攻撃的な戦略的意図の可能性があります。

2. リスク認識の差異（カスタム品特化型）: PAEは、一般的にiPhoneやWindows、あるいは自動車のように、数百万～数億台規模で販売される「高ボリューム（High Volume）」の汎用品を訴訟ターゲットにする傾向があります。ソシオネクストの現在の「Solution SoC」は、顧客ごとのカスタム品であり、製品ライフサイクルあたりの総量が（汎用品に比べ）限定的であるため、「自社はPAEのターゲットになりにくい」というリスク評価をしている可能性があります。
3. コスト対効果の判断: 単純に、LOT Networkの会費（事業規模に応じて変動）と、PAEから提訴されるリスク（＝ 提訴される可能性 × 想定損害額）を比較衡量し、現時点では加盟のコストメリット（リスク削減効果）がないと合理的に判断している可能性です。

いずれの仮説が真実であれ、主要顧客（全自動車メーカー）が全員加盟している防衛網に、その中核サプライヤーであるソシオネクストが加盟していないという事実は、両者のリスク戦略における注目すべき「非対称性」であり、同社の知財戦略における最大の特徴の一つであると言えます。

【比較表】主要ファブレス/IDMの知財戦略スタンス

比較軸	ソシオネクスト	**Broadcom**	**Marvell Technology**	**Renesas Electronics**
戦略モデル	Solution SoCの差別化・信頼獲得 [1]	市場の奪取・防衛 [2]	R&D/イノベーション主導 [3]	経営・事業戦略とIPの融合 [4]
ポートフォリオ	2nm/Chipletへの「集中」 [1]	高品質・訴訟活用 [2]	10,000件超の「量」と「質」 [3]	事業戦略連動 [4]
OSS対応	**OpenChain ISO**認証取得 [1]	(スニペット内情報なし)	(スニペット内情報なし)	(スニペット内情報なし)
PAE防衛	**LOT Network** 非加盟 [6]	活用重視（VMWare脱退） [5]	(スニペット内情報なし)	(スニペット内情報なし)
公表リスク	技術流出、OSS不適切利用、権利侵害 [1]	(スニペット内は主に訴訟当事者) [7]	(スニペット内は主に訴訟当事者) [8]	(スニペット内情報なし)

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 7. https://lotnet.com/press-releases/
- 9. https://pdaboards.memberclicks.net/index.php?option=com_dailyplanetblog&view=entry&year=2024&month=11&day=07&id=76:-renoirs-in-our-attics-
- 10. https://www.ipcg.com/cracking-the-code-caltechs-ongoing-patent-battle-with-apple-and-broadcom/
- 11. https://www.cloudcomputing-news.net/news/netflix-countersues-broadcom-over-vmware-patents/
- 12. https://arapackelaw.com/intellectual-property/source-code-intellectual-property/
- 13. https://www.marvell.com/company/newsroom/marvell-named-a-derwent-top-global-innovator-for-the-seventh-consecutive-year.html
- 39. http://www.jipa.or.jp/kaiin/kikansi/honbun/2010_03_0495.pdf
- 47. https://lotnet.com/members/
- 48. https://lotnet.com/lot-network-achieves-significant-membership-milestone-1000-members-and-counting/
- 49. https://en.wikipedia.org/wiki/LOT_Network

リスク・課題（短期/中期/長期）

ソシオネクストの知財戦略は、そのビジネスモデルに最適化されている一方で、特有のリスクと課題を内包しています。これらを時間軸（短期・中期・長期）で整理し、分析します。

短期リスク：第三者権利侵害（訴訟・係争）

同社が公式に認識する最大のリスクの一つが、「第三者の権利侵害に起因する訴訟・係争リスク」[1]

です。これは、同社にとって最も即時的かつ継続的な「短期リスク」であると考えられます。

カスタムSoCは、CPU、GPU、AIアクセラレータ、高速インターフェース、画像処理、通信機能など、極めて多数の機能・技術を単一のチップに集積します。この集積度と複雑度の高さは、必然的に、他社（競合、PAE、大学など）が保有する個々の要素技術（特許）に意図せず抵触してしまう（侵害してしまう）可能性を飛躍的に高めます。

特に、BroadcomがCaltech（カリフォルニア工科大学）と争った事例[10]や、MarvellがCMU（カーネギーメロン大学）から訴えられた事例[12]に見られるように、半導体業界は、一件の敗訴が巨額の賠償金（Marvellのケースでは一時11.7億ドル[12]）や、製品の販売差し止め（Injunction）に直結する、特許訴訟が非常に頻発する分野です。

このリスクは、SoCの機能が複雑化・高度化すればするほど増大する、いわば「宿命的なリスク」です。

この短期リスクに対し、ソシオネクストは、第2章で分析した「R&D（開発グループ）内に知財グループを配置する」[1]という組織体制によって、一定レベルのリスク管理（マネジメント）を行っていると推察されます。開発の初期段階から知財グループが関与し、他社特許の調査（クリアランス）や、侵害を回避する代替設計（デザイン・アラウンド）の検討、あるいは必要不可欠な特許のライセンスイン（導入）交渉を、R&Dと一体となって実行していると考えられます。これが、日常的なオペレーションにおける短期リスクへの主要な防衛策となっていると見られます。

中期リスク：技術・ノウハウの流出（ファブレスモデル）

同社が認識する「技術やノウハウの漏洩リスク」[1]は、より深刻な「中期リスク」であると考えられます。これは第4章で分析した通り、自社で工場を持たない「ファブレス」モデル[18]と、グローバルなサプライチェーン（ファウンドリ、OSAT）[17] [33]に起因する、構造的なリスクです。

このリスクは、サプライチェーンがグローバル化・複雑化するほど、また、製造委託先の数が増え、その所在地が法執行の目が届きにくい国・地域に広がるほど、管理が困難になり増大します。

特に、ソシオネクストが現在R&Dリソースを集中投下している「2nm/チップレット」[1]という最先端技術は、設計ノウハウの塊であり、その経済的価値は計り知れません。これらの技術・ノウハウ（＝企業秘密、トレードシークレット）の漏洩リスクの管理（第4章で述べた法的・物理的・技術的防衛）がもし失敗した場合、その損害は計り知れません。

それは、単なるライセンス料の逸失や、短期的な訴訟問題（短期リスク）に留まりません。ソシオネクストの「差別化の源泉」[1]であり、顧客に「Solution SoC」として提供する価値の根幹である最先端ノウハウが、競合他社や、あるいは（過剰生産等を通じて）市場全体に拡散することを意味します。これは、同社のビジネスモデルの根幹を揺るがす、致命的な打撃となる可能性を秘めた中期的なリスク

です。

長期リスク：**PAE**（特許トロール）による訴訟

第6章で詳述した通り、ソシオネクストはPAE（パテント・トロール）に対する強力な防衛網である「LOT Network」に加盟していません（[6]の調査結果）。この「非加盟」という戦略的選択は、同社の知財戦略における最大の「長期リスク」であると分析されます。

第6章で挙げた仮説のうち、仮に「（現時点では）カスタム品で低ボリュームだからPAEのターゲットになりにくい」（仮説2）というリスク評価が正しいとしても、それはあくまで「現時点」での話です。

ソシオネクストの事業が今後さらに拡大し、特に「Automotive（車載）」や「Data Center（データセンター）」の分野で同社が開発した「Solution SoC」が、その性能と信頼性（OSSの信頼性[1]を含む）の高さから、複数の顧客に採用され、業界の「デファクト・スタンダード（事実上の標準）」的な地位を獲得した場合、そのSoCは「低ボリューム」ではなく「高ボリューム」製品へと変貌します。

そうなった場合、同社はPAEにとって、またとない魅力的な訴訟ターゲットとなります。

この長期リスクが顕在化した場合、LOT Networkに加盟している競合他社や、同社の顧客である自動車メーカー全社[48] [49]は、コミュニティの防衛機能によって自動的に守られます。一方で、ソシオネクストは、その防衛網の外で、単独でPAEの攻撃に立ち向かい、巨額の訴訟費用とライセンス料（あるいは事業停止）のリスクに直面することになります。

この「非加盟」という戦略的選択は、現時点でのコスト削減や戦略的自由度（仮説1, 3）を優先する一方で、将来の成功（＝高ボリューム化）によって自らリスクを引き寄せるという、長期的な時限爆弾を抱える可能性を示唆しています。これは、同社の知財戦略における最大のリスク・アペタイト（許容するリスク）の発現点であると分析されます。

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 10. https://www.ipcg.com/cracking-the-code-caltechs-ongoing-patent-battle-with-apple-and-broadcom/
- 12. https://arapackelaw.com/intellectual-property/source-code-intellectual-property/
- 17. https://gigazine.net/news/20181129-dynamic-camouflaging-approach-on-chip/
- 18. https://hasegawa-kakosho.com/faburesukigyou/

- 33. https://gigazine.net/news/20181129-dynamic-camouflaging-approach-on-chip/
- 48. https://lotnet.com/lot-network-achieves-significant-membership-milestone-1000-members-and-counting/
- 49. https://en.wikipedia.org/wiki/LOT_Network

今後の展望（政策/技術/市場動動との接続）

ソシオネクストの知財戦略は、外部環境の大きな変化、特に「欧州における特許司法制度の激変」と「AI技術の爆発的普及」という二つのトレンドによって、新たな機会と脅威に直面すると予想されます。

欧州統一特許裁判所（UPC）への対応

2023年6月1日、欧州において「統一特許裁判所（UPC：Unified Patent Court）」が発足しました[34]。これは、欧州の特許戦略における過去数十年で最大の地殻変動であり、同社のグローバルな知財戦略に重大な影響を与えます。

UPCは、欧州における特許訴訟のあり方を根本的に変えるものです。従来、欧州で特許侵害訴訟を行う場合、特許権者は国ごと（ドイツ、フランス、イタリアなど）に個別に訴訟を提起し、判決を得る必要がありました。これには莫大な時間と費用がかかっていました[19]。

しかし、UPCの発足により、単一の訴訟手続きで、UPC協定に加盟する全18カ国（2024年9月時点、ドイツ・フランス・イタリア・オランダなど主要国を含む[37]）全域において、特許侵害の差し止めや損害賠償を命じる判決を得ることが可能になりました[35] [36]。実際に2024年10月には、非欧州企業である韓国のソウル半導体が、このUPCで勝訴し、侵害製品に対して8カ国での販売禁止・リコール・製品破壊という、極めて強力な判決を獲得しています[19]。

このUPCの登場は、第3章で分析したソシオネクストの「外国出願の積極的推進」[1]戦略、特に欧州（主要な自動車メーカーが集中する市場）戦略に対し、二律背反（トレードオフ）の展望をもたらします。

1. オフェンス（機会）：これは、ソシオネクストにとって極めて強力な「攻め」の武器となり得ます。同社が注力する「2nm/チップレット」[1]に関する欧州特許（あるいはUPCで一元的に管轄される「ユニタリ特許」）を1件でも取得・維持できれば、その1件の特許を行使するだけで、競合他社に対

し、欧州の主要18カ国全域での製造・販売を一挙に差し止めるという、絶大なレバレッジ（交渉力）を持つことができます。

2. ディフェンス（脅威）：逆に、この力はPAEや競合他社にとっても同様です。ソシオネクストが、PAEや競合からUPCで特許侵害で提訴された場合、単一の訴訟で敗訴するだけで、欧州の全主要市場（特に自動車市場）から一斉に締め出される（販売差し止めを命じられる）という、事業継続に関わる壊滅的なリスクを負うことになります。

このUPCという「ハイリスク・ハイリターン」な司法制度の登場は、第7章で論じたPAEリスク（LOT Network非加盟）を、欧州市場において特に増幅させる要因となります。今後の同社の欧州特許戦略は、このUPCの特性（機会）を最大限に活用しつつ、同時に最悪の事態（脅威）を回避する（例えば、自社の既存の重要特許をUPCの管轄から除外する「オプトアウト」戦略の戦術的検討など）精緻なものが、早急に求められると予想されます。

AIとSoCの融合、そしてOSSリスクの増大

今後の技術トレンドとして、AI（人工知能）、特に生成AI（GenAI）のアクセラレータ（推論や学習を高速化する専用回路）をSoCに統合する動きが、あらゆる分野（データセンター、車載、スマートデバイス）で爆発的に加速しています[42]。

このAI技術の進化と普及は、OSS（オープンソース）の利用と表裏一体です。現代のAI/機械学習の分野は、GoogleのTensorFlowやMetaのPyTorchに代表される、OSSのライブラリやフレームワークの利用が最も活発な分野の一つです。

このトレンドは、ソシオネクストの知財戦略、特に第5章で分析したOSSコンプライアンス戦略にとって、二重の意義を持ちます。

第一に、ソシオネクストがAI搭載の「Solution SoC」開発を推進すればするほど、必然的に、SoCに組み込まれるソフトウェア・スタックに含まれるOSSの量と種類は、爆発的に増加すると予想されます。

第二に、これは、同社の「ソフトウェア管理推進グループ」[1]と、取得済みである「OpenChain ISO/IEC 5230:2020」認証[1]体制が、今後さらにその戦略的重要性を増すことを意味します。

AI関連のOSSは、開発スピードが速い反面、複雑なライセンス（例：AGPLなど、ネットワーク経由での利用でもソースコード開示義務が生じる可能性のあるもの）を含んでいたり、日々新たな脆弱性が発見されたりする、管理が非常に難しいソフトウェア群です。

第5章で指摘したように、半導体業界はもともとOSSのリスク管理が極めて不十分な業界（脆弱性88%、ライセンス競合92%[23]）です。競合他社が、このAI時代に急増するOSSの管理（いわば「技術的負債」の清算）にこれから着手し、苦慮する可能性が高い中で、ソシオネクストは既に「ISO認証」という国際標準の管理プロセスを確立・運用しているという、明確な先行者利益（アドバンテージ）を持っ

ています。

同社のこの先行投資は、AI時代におけるSoCベンダーの必須の競争力（＝信頼性）となり、他社がOSSの「負債」に苦しむ中で、同社はOSSの「利便性」を最大限に享受し、信頼性の高いAI-SoCを迅速に市場に投入することを可能にすると考えられます。

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 19. https://vision00.jp/topic/10365/
- 23. https://www.synopsys.com/ja-jp/japan/press-releases/2024-04-17-2.html
- 34. https://www.unifiedpatentcourt.org/en
- 35. https://www.mwe.com/resource/unified-patent-court-resource-center/
- 36. https://www.epo.org/en/applying/european/unitary/upc
- 37. https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/patent-protection-eu/unitary-patent-system_en
- 42. https://henry.law/blog/semiconductor-technology-an-overview-of-the-global-patent-landscape/

戦略的示唆（経営/研究開発/事業化の観点でアクション候補）

本レポートで実施した網羅的分析に基づき、ソシオネクストがその知的財産戦略の価値を最大化し、内在するリスクを最小化するために、今後検討し得る戦略的なアクション候補を、経営、研究開発（R&D）、事業化（マーケティング）の三つの観点で以下に示します。

経営観点（リスク・アペタイトの再定義）

- アクション候補：**LOT Network**への加盟に関する戦略的再評価
- 根拠: 第6章で詳細に分析した通り、ソシオネクストは現在、PAE（パテント・トロール）防衛網であ

る「LOT Network」に加盟していません（[6]の調査結果）。これは、同社の主要顧客（特に「世界の上位7社の自動車メーカー」全社[48] [49]）が加盟しているという事実と、明確に逆のスタンスです。この「非対称性」は、ソシオネクストが単独でPAE訴訟リスクを負うことを意味し、第7章で指摘した通りの「長期リスク」を構成しています。

- 示唆: 経営陣は、この「非加盟」という現在のスタンスについて、戦略的な再評価を行うことが推奨されます。具体的には、「PAE訴訟リスクの低減（＝加盟メリット）」と、「特許活用の戦略的自由度の確保（例：特許売却益）および会費コスト（＝非加盟メリット）」を、天秤にかける必要があります。この比較衡量（トレードオフ）は、以下の三つの変化点を踏まえて行われるべきです。
  1. 事業規模の変化**:** 同社の事業が拡大し、SoCが「高ボリューム」化するにつれ、PAEのターゲットになるリスクは非線形に増大します。
  2. 司法環境の変化**:** 第8章で分析した欧州UPC[34]の発足は、欧州における訴訟リスクを（特に非加盟企業にとって）劇的に高めました。
  3. 顧客関係の変化: 主要顧客（自動車メーカー）[48]が加盟する防衛網にサプライヤーとして非加盟であり続けることが、顧客とのリスク分担において、どのような（潜在的な）不協和音を生む可能性があるか。

     経営陣は、これらを踏まえ、「非加盟を継続する」という判断を下す場合においても、それが「積極的な戦略的選択」であることを確認し、PAEから（特にUPCなどで）提訴された場合に単独で対抗するための十分な訴訟防衛予算と戦略（カウンター用の特許ポートフォリオ）を、意識的に準備しておく必要があると推察されます。

研究開発観点（**R&D**プロセスの高度化）

- アクション候補①： ハードウェア**IP**防衛策（トレードシークレット）の継続的強化
- 根拠: 第4章で分析した通り、ファブレスモデルにおける「技術・ノウハウの漏洩」[1]は、同社のビジネスの根幹を揺るがす最大のリスク（中期リスク）の一つです。
- 示唆: サプライチェーン（ファウンドリ、OSAT）における厳格な契約管理やアクセス管理（法的・物理的防衛）に加え、R&D（開発グループ）の設計段階で、リバースエンジニアリングやハードウェア・トロイの木馬による改ざんを「技術的」に困難にする手法（例：[10]で言及される「動的カモフラージュ」や回路難読化、PUFなど）の研究開発と実装を、R&D（開発グループ）内の知財グループ[1]と連携して、継続的に推進することが求められます。OSS（ソフトウェア）の防衛（第5章）が「公開（ISO認証）」であるのに対し、ハードウェアの防衛は「秘密（トレードシークレット）」であり、両輪での強化が不可欠です。
- アクション候補②： **R&D**と知財グループの連携による「**UPC**最適化」出願戦略の策定
- 根拠: 第8章で分析した通り、UPC[34]の発足は、欧州特許の価値（レバレッジ）とリスク（差し止め）を根本的に変えました。
- 示唆: この新しいゲームのルールに対応するため、R&D（開発グループ）と、その内部に存在する知財グループ[1]は、緊密に連携する必要があります。具体的には、発明ごと（特に「2nm/チップレット」[1]関連）に、「この発明はUPCで戦う『攻め』の特許か、それともUPCで攻撃されたくない『守り』の特許か」を判断し、出願形式（伝統的欧州特許かユニタリ特許か）や、UPCの管轄から除外する「オプトアウト」の是非を、一件ごとに戦略的に判断・実行する、極めて高度な実務プロ

セスを策定・実行する必要があると考えられます。

事業化観点（「信頼」のマーケティング）

- アクション候補：「**OpenChain ISO/IEC 5230:2020**」認証の積極的なマーケティング活用
- 根拠: 第5章で分析した通り、半導体業界はOSSの脆弱性・ライセンス違反リスクが全業界で最悪[23]であり、顧客（特に車載・データセンター）の懸念が最も大きい分野です。
- 示唆: ソシオネクストは、この業界最大のリスクに対し「国際標準（ISO）認証の取得」[1]という、客観的かつ具体的な「解」を持っています。これは、単なる「コンプライアンス部門（守り）」の成果に留めておくべきではありません。
  むしろ、営業・マーケティング部門が、これを「攻め」のツールとして積極的に活用すべきです。顧客（特に新規の車載メーカーや金融・通信向けデータセンター事業者）に対し、「他社のSoCは、92%がライセンス違反、88%が脆弱性のリスク[23]を抱えた『ブラックボックス』かもしれないが、当社のSoCは、ソフトウェア・サプライチェーンの『信頼性』がISOレベルで保証されている」という、客観的データに基づいた強力な差別化要因としてアピールすべきです。これにより、技術仕様（スペック）競争だけでは超えられない「信頼」の壁を越え、NRE契約の獲得（＝事業化）を強力に後押しできると推察されます。

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 5. https://lotnet.com/members/ [6]
- 23. https://www.synopsys.com/ja-jp/japan/press-releases/2024-04-17-2.html
- 33. https://gigazine.net/news/20181129-dynamic-camouflaging-approach-on-chip/
- 34. https://www.unifiedpatentcourt.org/en
- 48. https://lotnet.com/lot-network-achieves-significant-membership-milestone-1000-members-and-counting/
- 49. https://en.wikipedia.org/wiki/LOT_Network

総括

本レポートは、株式会社ソシオネクストの知的財産戦略について、公開されている一次情報を基に網羅的に分析しました。

導き出された最重要論点は、同社の知財戦略が、その独自の「Solution SoC」ビジネスモデル[1]と、R&D部門（開発グループ）に知財部門を組み込む（Embedする）という「組織体制」[1] [31]によって、極めて合理的に最適化されているという点です。これは、知財を単なる法務機能ではなく、R&DおよびビジネスとI一体化した「価値創出の源泉」[1]と定義する同社の方針を具現化したものと言えます。

具体的には、①「2nm/チップレット」という最先端分野への特許出願の「集中」[1]、②NRE収益に連動した「グローバル」出願の推進[1]、③半導体業界最悪[23]とも言われるOSSリスクに対する「OpenChain ISO認証」[1]取得という高度なコンプライアンス体制の構築、という三つの柱が確認されました。特に③は、リスク（守り）を、顧客からの「信頼（攻め）」に転換する、他社にはない優れた戦略的対応と高く評価されます。

一方で、本分析における最大の戦略的課題は、PAE（パテント・トロール）防衛網である「LOT Network」への「非加盟」[5]（[6]の調査結果）というスタンスです。これは、主要顧客である自動車メーカー全社[48]が加盟する中で顕著な「非対称性」であり、同社の事業規模が拡大し、欧州UPC[34]のような訴訟環境が激化する中で、長期的な訴訟リスクを高める可能性を内包しています。

経営上の意思決定への含意として、この「非加盟」スタンスが、コスト回避やリスク認識の差異に基づく現状維持（受動的判断）なのか、あるいは特許活用（例：売却益）の自由度を確保するための「積極的判断」なのかを明確にし、後者であれば単独での訴訟防衛体制の強化を、前者であれば加盟の是非を、外部環境の変化（UPC、AIの台頭）を踏まえて再評価することが、今後の持続的成長における重要な論点となると推察されます。

当章の参考資料

- 1. https://www.socionext.com/en/sustainability/IP/
- 5. https://lotnet.com/members/ [6]
- 23. https://www.synopsys.com/ja-jp/japan/press-releases/2024-04-17-2.html
- 31. https://www.socionext.com/jp/download/catalog/AD00-00006-2.pdf
- 34. https://www.unifiedpatentcourt.org/en
- 48. https://lotnet.com/lot-network-achieves-significant-membership-milestone-1000-members-and-counting/

参考資料リスト（全体）

- 1. https://www.socionext.com/en/sustainability/IP/
- 2. https://www.socionext.com/en/download/catalog/AD00-00006-2E.pdf
- 3. https://www.socionext.com/en/download/catalog/AD00-00006-1E.pdf
- 4. https://www.socionext.com/en/ir/
- 5. https://www.socionext.com/en/sustainability/ESG_Report/
- 6. https://www.socionext.com/jp/download/catalog/AD00-00006-2.pdf
- 7. https://lotnet.com/press-releases/
- 8. https://www.iprcenter.gov/file-repository/ipec-2020-annual-intellectual-property-report-1.pdf
- 9. https://pdaboards.memberclicks.net/index.php?option=com_dailyplanetblog&view=entry&year=2024&month=11&day=07&id=76:-renoirs-in-our-attics-
- 10. https://www.ipcg.com/cracking-the-code-caltechs-ongoing-patent-battle-with-apple-and-broadcom/
- 11. https://www.cloudcomputing-news.net/news/netflix-countersues-broadcom-over-vmware-patents/
- 12. https://arapackelaw.com/intellectual-property/source-code-intellectual-property/
- 13. https://www.marvell.com/company/newsroom/marvell-named-a-derwent-top-global-innovator-for-the-seventh-consecutive-year.html
- 14. https://www.uspto.gov/about-us/events/public-symposium-ai-and-ip
- 15. https://www.manufacturersalliance.org/sites/default/files/2021-06/Beyond%20Patents-%20IP%20Strategy%2C%20Valuation%2C%20and%20Management%20in%20Manufacturing.pdf
- 16. https://featured.com/questions/ip-strategy-example-industry-lessons

- 17. https://gigazine.net/news/20181129-dynamic-camouflaging-approach-on-chip/
- 18. https://hasegawa-kakosho.com/faburesukigyou/
- 19. https://vision00.jp/topic/10365/
- 20. https://patents.google.com/patent/US8738860B1/en
- 21. https://patents.google.com/patent/EP2101455A2/zh
- 22. https://portal.unifiedpatents.com/patents/patent/US-10530839-B2
- 23. https://www.synopsys.com/ja-jp/japan/press-releases/2024-04-17-2.html
- 24. https://www.denso.com/global/en/-/media/global/about-us/investors/annual-report/2025/annual-report-doc-2025-viewing-en.pdf?la=en&rev=6468750bd910437e8901bf7d7d306283&hash=AEE043DF8C30A99679085A1BB6C8E500
- 25. https://www.minebeamitsumi.com/english/corp/investors/disclosure/integrated_report/a2025/__icsFiles/afieldfile/2025/11/04/2025_integrated_report_en.pdf
- 26. https://www.nec.com/en/global/ir/pdf/annual/2024/ar2024-e.pdf
- 27. https://www.mitsubishielectric.com/investors/library/integrated-report/pdf/2024/integrated_report2024_en.pdf
- 28. https://global.fujitsu/-/media/Project/Fujitsu/Fujitsu-HQ/about/integrated-report/2025/integrated-report-2025-en.pdf
- 29. https://www.skadden.com/sitemap/insights
- 30. https://www.btlj.org/data/articles2016/vol31/31_3/4-Chien_JCI.pdf
- 31. https://www.socionext.com/jp/download/catalog/AD00-00006-2.pdf
- 32. https://www.nedo.go.jp/content/100927040.pdf
- 33. https://gigazine.net/news/20181129-dynamic-camouflaging-approach-on-chip/
- 34. https://www.unifiedpatentcourt.org/en
- 35. https://www.mwe.com/resource/unified-patent-court-resource-center/

- 36. https://www.epo.org/en/applying/european/unitary/upc
- 37. https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/patent-protection-eu/unitary-patent-system_en
- 38. https://www.cooley.com/news/insight/2022/2022-09-12-a-guide-to-the-unitary-patent-system-and-unified-patent-court
- 39. http://www.jipa.or.jp/kaiin/kikansi/honbun/2010_03_0495.pdf
- 40. https://patent-i.com/report/jp/applicant/0000164/
- 41. https://orbit.dtu.dk/files/332405588/J_of_Product_Innov_Manag_2023_Wambsganss.pdf
- 42. https://henry.law/blog/semiconductor-technology-an-overview-of-the-global-patent-landscape/
- 43. https://www.eetimes.com/how-strong-are-your-ip-assets/
- 44. https://unitedlex.com/insights/the-auto-industrys-need-for-a-drastic-ip-strategy-reset/
- 45. https://www.hitachi.com/about/activity/ip/2008/nrdip2008.pdf
- 46. https://lotnet.com/
- 47. https://lotnet.com/members/
- 48. https://lotnet.com/lot-network-achieves-significant-membership-milestone-1000-members-and-counting/
- 49. https://en.wikipedia.org/wiki/LOT_Network
- 50. https://www.onetrust.com/news/onetrust-joins-lot-network/
- 51. https://www.sompo-hd.com/-/media/hd/files/csr/communications/pdf/2023/report2023.pdf?la=ja-JP
- 52. https://www.socionext.com/en/ir/pdf/sn_ir20250829_01e.pdf
- 53. https://www.socionext.com/en/pr/sn_pr20150302_01e.pdf

- 54. https://www.fujitsu.com/global/about/resources/news/press-releases/2015/0302-02.html
- 55. https://www.sec.gov/Archives/edgar/data/63271/000119312515243551/d948256d6k.htm

引用文献

1. Intellectual Property | Sustainability | Socionext Inc., 11月 7, 2025にアクセス、https://www.socionext.com/en/sustainability/IP/
2. "Renoirs in our Attics" - Private Directors Association, 11月 7, 2025にアクセス、https://pdaboards.memberclicks.net/index.php?option=com_dailyplanetblog&view=entry&year=2024&month=11&day=07&id=76:-renoirs-in-our-attics-
3. Marvell Named a Derwent Top 100 Global Innovator for the Seventh Consecutive Year, 11月 7, 2025にアクセス、https://www.marvell.com/company/newsroom/marvell-named-a-derwent-top-global-innovator-for-the-seventh-consecutive-year.html
4. 株式会社ルネサステクノロジ - 日本知的財産協会, 11月 7, 2025にアクセス、http://www.jipa.or.jp/kaiin/kikansi/honbun/2010_03_0495.pdf
5. Press releases - LOT Network, 11月 7, 2025にアクセス、https://lotnet.com/press-releases/
6. Meet The Companies That Make Up The LOT Network Community, 11月 7, 2025にアクセス、https://lotnet.com/members/
7. Cracking the Code: Caltech's Ongoing Patent Battle with Apple and Broadcom - ipCG, 11月 7, 2025にアクセス、https://www.ipcg.com/cracking-the-code-caltechs-ongoing-patent-battle-with-apple-and-broadcom/
8. Strategies for Protecting Source Code Intellectual Property - The Rapacke Law Group, 11月 7, 2025にアクセス、https://arapackelaw.com/intellectual-property/source-code-intellectual-property/
9. Annual Securities Report - Socionext Inc., 11月 7, 2025にアクセス、https://www.socionext.com/en/ir/pdf/sn_ir20250829_01e.pdf
10. 知財窃盗や悪意あるコード混入などを予防するため半導体チップを動的にカモフラージュする技術が考案される - GIGAZINE, 11月 7, 2025にアクセス、https://gigazine.net/news/20181129-dynamic-camouflaging-approach-on-chip/