THE LINUX FOUNDATION | Research

OSPO価値の測定：投資収益率(ROI)、レジリエンス、リスク予測、戦略的影響力のためのフレームワーク

経営幹部、OSPO実践者、

および技術戦略担当者向けレポート

Ibrahim Haddad, *PhD*

序文

Ana Jiménez Santamaría, *The Linux Foundation*

2026年6月

提携

TODO

OSPOの価値測定：ROI、レジリエンス、リスク予測、戦略的影響力のためのフレームワーク

オープンソースは、現代の企業における***製品、インフラストラクチャ、および業務運営***を支えています。

OSPOのパフォーマンスは、活動件数やワークフローの量ではなく、***ビジネス成果***によって評価されるべきです。

OSPOの価値は、さまざまな形態の企業価値を捉える*指標のポートフォリオ*として測定するのが最適です。

OSPOの測定が不十分だと、***投資不足、ガバナンスの範囲の誤り***、戦略的な盲点につながります。

信頼できるOSPO評価指標は、経済性、準備態勢、先見性、戦略的影響力のバランスを取るべきです。

OSPOは、企業全体の*ガバナンス、可視性、意思決定の質*を向上させることで価値を創造します。

レジリエンスとは、組織が混乱によって***即興的な対応や高額な費用のかかる事後処理***を強いられる前に、準備を整えておくことを意味します。

強力なOSPOガバナンスは、文書化や追跡だけでなく、***明確な意思決定とコミュニケーション***にかかっています。

組織は、依存しているオープンソースのエコシステムに***積極的に参加する***ことで、***より大きな影響力***を得ることができます。

OSPOの価値を適切に測定できる組織は、摩擦を減らし、***より良いオープンソースに関する意思決定***を行うことができます。

AIが生成したコードは、標準的なコンプライアンスワークフローでは対応できない新たな***ガバナンス上の複雑さ***を加えます。

OSPOにおけるリスク予測とは、問題がまだ対処可能な段階で、***発生しつつある問題を検知すること***を意味します。

目次

序文.....04
エグゼクティブ サマリー.....05
導入.....06
OSPOSの価値を測定する緊急性.....07
測定のための設計原則.....09
4次元OSPO価値フレームワーク.....10
次元1：投資対効果（ROI）とコスト回避.....14
次元2：レジリエンス.....16
次元3：リスク予測.....18
次元4：戦略的影響力.....20
信頼性の高いOSPO価値測定システム構築のための原則.....22
経営幹部向け報告モデル.....23
OSPOの進化に伴い、測定方法も進化する.....26
実践的な導入ロードマップ.....28
結論：OSPOの物語を再構築する.....30
付録A. OSPO評価基準カタログ.....31
リソース.....38
フィードバック.....39
謝辞.....39
免責事項.....39
著者について.....40

序文

テクノロジー業界全体で根本的な変化が起きています。インフラストラクチャはもはや、バックグラウンドで静かに稼働する目に見えない層ではなく、組織の価値、レジリエンス、そして長期的な競争力を決定づける戦略的な要素となっています。

この変化が最も顕著に表れているのがAI分野です。モデル コンテキスト プロトコル（MCP）やA2A（エージェント間）プロトコルといったオープンなプロトコルや相互運用性標準、Gooseなどのオープンソースのエージェント ツール、そしてHermesやOpenClawといった新興のオープンソース エージェント プラットフォームは、組織がAIを活用したシステムを開発、接続、運用するための基盤となる構成要素になりつつあります。

このような状況において、オープンソースは、ビジネス能力、リスク領域、ガバナンス上の課題、そして組織が意図的に参加する戦略的環境へと変化しました。

これにより、Open Source Program Office（OSPO）の役割がますます重要性を増しています。こうしたエコシステムが成熟するにつれ、組織は、何に依存しているのか、それらの技術がどのように管理されているのか、リスクはどこで発生する可能性があるのか、そして受動的な依存ではなく長期的な価値を生み出す形でどのように参加できるのかを理解するための機能を必要としています。OSPOとそのオープンソース専門家は、こうした現実を結びつけるのに最適な立場にあります。

しかし、OSPOの価値を伝えるのはしばしば困難でした。多くの場合、チケットの完了数、リポジトリのスキャン数、貢献依頼のレビュー数、トレーニングの実施数といった活動件数で説明されてきました。これらの指標は役立つ場合もありますが、OSPOがビジネスにとってなぜ重要なのかを十分に説明するものではありません。

だからこそ、このレポートは時宜を得たものと言えるのです。オープンソース管理を、組織が事業運営に必要な能力、すなわちコスト効率、運用上のレジリエンス、リスク予測、そして組織のインフラストラクチャを形成するオープン エコシステムにおける戦略的影響力と結びつけているからです。

オープンソース開発者コミュニティや、組織内でオープンソース管理を担当する実務担当者との協働を通して、このニーズがますます切迫していることを実感してきました。OSPO（Open Source Program Office）には、経営陣が行動に移せるようなフレームワークが必要です。それは、OSPOが何をするのかだけでなく、組織にどのような価値をもたらすのかを説明するものでなければなりません。

新たなエージェント型ワークフロー、オープン プロトコル、相互運用性標準、オープンソースAIツールの登場により、新たな依存関係とガバナンス上の課題が生じるため、このニーズはますます切迫したものとなっています。OSPO（オープンソース·セキュリティ·オペレーション）にとっての課題は、導入を支援するだけでなく、より良い意思決定、より強固なレジリエンス、より明確なリスク管理、そしてより戦略的なエコシステムへの参加を通じて、組織に測定可能な価値をもたらすことを示すことです。本レポートは、こうした変化を可視化し、測定可能で、実行可能なものにするための実践的な基盤を提供します。

Ana Jiménez Santamaría、
Senior Project Manager、
The Linux Foundation

エグゼクティブ サマリー

本レポートでは、Open Source Program Office（OSPO）のビジネス価値を、コスト効率、運用上のレジリエンス、リスク予測、戦略的影響力という4つの側面から測定するための構造化された手法を提案しています。参照モデル フレームワークは、明確な因果関係を通じてOSPOの活動を測定可能なビジネス成果に結び付けます。活動指標、運用成果、財務的価値またはリスク調整済み価値を区別します。例えば、SBOMのカバー率を高めることで脆弱性検出速度が向上します。検出速度が速くなると修復までの平均時間が短縮され、本番環境におけるインシデントの発生確率と影響が低減します。その結果、組織は停止コストを回避したり、セキュリティ リスクを軽減したりすることができます。このフレームワークは、経営幹部の意思決定を支援するために設計されています。これは、組織がOSPOへの貢献度を定量化し、投資と成果を比較し、OSPOの指標をより広範なエンジニアリングおよびリスク ダッシュボードに統合するために適用できるベースライン モデルを提供します。

導入

オープンソース ソフトウェアは、現代のソフトウェア システムの大部分に組み込まれています。業界調査によると、ほとんどの商用コード ベースは、外部で保守されているオープンソース コンポーネントに依存していることが一貫して示されています。この依存関係は、影響力とリスクの両方をもたらします。最近のセキュリティ インシデントは、広く使用されているコンポーネントの脆弱性が業界全体に急速に広がる可能性があることを示しています。こうした状況により、オープンソースは単なる技術的な懸念事項から、取締役会レベルのリスクと戦略に関する重要なテーマへと位置づけられるようになりました。

組織はこうした複雑な問題に対処するためにOSPO（組織的組織方針）を策定している。しかし、ほとんどのOSPOは、貢献度や方針の採用状況といった活動ベースの指標を用いて評価されている。これらの指標はビジネス価値を明確に示すものではありません。本レポートは、OSPOの活動をビジネス成果および定量化可能な影響に結びつける測定フレームワークを定義することで、このギャップを埋めます。

企業におけるオープンソース ソフトウェアへの依存度が高まるにつれ、そのエコシステムとの連携やガバナンスの調整の必要性も高まっています。OSPO（オープンソース ソフトウェア組織）は、こうした現実に対応するために誕生しました。最も基本的な形態では、OSPOはポリシー、プロセス、トレーニング、ツール、コンプライアンス サポートを提供します。より成熟したレベルでは、OSPOは貢献戦略、開発者支援、サプライヤーの期待、エコシステムへの参加、そしてオープンソースのリスクと機会に関する経営陣の可視性も形成します。

しかし、OSPOの価値を測定することは、少なくとも4つの理由から、これまで困難でした。

- **OSPOの価値の多くは予防的である**：OSPOがソフトウェア リリース前にライセンスの問題を特定したり、依存関係の取り込みパスを改善したり、ガバナンス上の懸念を早期に検出したりすると、結果として、目に見える形でエスカレートし、コストのかかる事態ではなく、危機を回避できることがよくあります。
- **効果は分散される**：OSPOの恩恵は製品チーム、エンジニアリング業務、法務、セキュリティ、調達、戦略といった部門が、単一の予算項目ではなく、それぞれ独立した組織として関わっています。これらの影響を把握することは容易ではありません。
- **その影響は複数期間に及ぶ**：審査サイクルの短縮など、四半期以内に現れるメリットもあれば、エコシステムへの影響や囲い込みの軽減など、数年かけて現れるメリットもあります。
- **この仕事は部門横断的である**：OSPOの成果は、技術、法律、運用、文化（コミュニティ）、戦略といった様々な側面から構成されます。

問題は、意思決定者や経営幹部スポンサーにOSPOの価値を明確に伝える言葉が不足していることにある場合が多い。信頼できる測定モデルまたはOSPO価値フレームワークが必要である。2つの制約を満たす必要があります。1つは、経営陣による審査と優先順位付けを支えるのに十分な厳密さを備えていること、もう1つは、オープンソースガバナンスの真の特性を反映する柔軟性を備えていることです。

こうした測定の難しさには、構造的な要因も含まれています。OSPOの価値は、予防的であり、組織全体に分散し、部門横断的に作用するからです。また、組織的な要因も関係しています。多くの企業は、その価値を確実に把握するために必要なデータ経路、報告体制、部門横断的な計測ツールをまだ構築していないのです。この区別は重要です。なぜなら、不完全な可視性は、影響力の欠如とは異なることをリーダーに認識させるからです。

OSPOSの価値を測定する緊急性

オープンソースの運用環境がここ数年で大きく変化したため、OSPOの価値を測定することがより喫緊の課題となっています。以下のサブセクションでは、あらゆる企業においてOSPOが価値を実証するよう促す5つの主要な要因を探ります：

- オープンソースは、収益に直結するシステムにより近い位置づけになった
- セキュリティとサプライ チェーンに対する期待が高まっている
- オープンソース ソフトウェアに影響を与える規制の強化
- リーダーシップに対する期待の変化
- AI生成コードによりガバナンスの複雑さが増した

オープンソースは今や収益に直結するシステムにより近い位置付けになった

製品のソフトウェア定義化が進むにつれ、オープンソースへの依存は、顧客体験、リリース信頼性、セキュリティ体制、および運用継続性に直接影響を与えるようになっています。このような環境は、OSPO（オープンソース ソフトウェア最適化）パフォーマンスの重要性を変化させています。オープンソースは、製品の提供速度、修復品質、そして技術的負債への潜在的なリスクを蓄積することなく迅速に行動できる企業の能力に影響を与えるようになっています。

セキュリティとサプライ チェーンに対する期待が高まっている

OSPOの機能は現在、オープンソース コンプライアンス、貢献管理、依存関係の透明性、脆弱性対応の調整、SBOMワークフロー、およびより広範なサプライ チェーンの準備状況を網羅しています。この範囲と責任の移行は、SBOMとソフトウェア サプライチェーン ガバナンスに関する公開ガイダンスによってさらに強化されており、透明性とトレーサビリティは、例外的な慣行ではなく、責任あるソフトウェア管理の通常の要素としてますます扱われるようになっています。

規制の増加

2024年12月10日に発効した**欧州連合のサイバー レジリエンス法**（CRA：Cyber Resilience Act、EU規則2024/2847）は、近年のオープンソース ガバナンスに関する最も重要な規制上の進展です。この規則は、EU市場で販売されるデジタル要素を含む製品に対するサイバーセキュリティ要件を義務付けており、組織がオープンソースへの依存を管理する方法に直接的な影響を与えます。具体的には、脆弱性開示の期限、SBOM（ソフトウェア部品表）の透明性、適合性評価、およびEU市場に製品を投入する商用オープンソース インテグレーターの取り扱いに関する義務を定めています。

CRAは、オープンソースを含む製品を商用サプライチェーンに組み込む行為を規制するものです。これにより、ガバナンスに関する期待は、上流のコミュニティから、それらのコンポーネントを統合して出荷する企業へと移行します。文書化された導入プロセス、依存関係のインベントリ、脆弱性対応ワークフローを持たない組織は、CRAの義務が段階的に導入されるにつれて、商業的および運用上のリスクに直面することになります。悪用された脆弱性を報告する製造業者の義務は2026年9月11日から適用され、すべての義務は2027年12月11日から適用されます。

OSPOが構築するガバナンス インフラストラクチャ、依存関係の可視化、SBOMの実践、コミュニティとの連携、上流との関係管理、脆弱性対応の調整などは、規制当局、企業顧客、保険引受会社が基本的な期待事項として扱うようになっているインフラストラクチャとますます同じものになりつつあります。

OSPOスコアカードを通じてCRA（地域再投資法）への対応能力を証明しようとする組織は、特に以下の4つの指標に注意を払うべきです：

- SBOMのカバー率（付録A.3）は、CRAの透明性義務に直接対応しています
- 上流の問題に対する認識までの時間（付録A.3）は、脆弱性通知のタイムラインに関連しています
- リリース前に高リスクな問題が特定されたことは（付録A.4）、積極的なガバナンスの証である。リリース前に高リスク問題が特定された。これは積極的なガバナンス体制を示しています
- コンプライアンス サイクル タイムの短縮（付録A.2）は、機能的な受付プロセスの証拠となります

これら4つの指標は、顧客、監査人、または規制当局とのCRA（信用リスク評価）に焦点を当てたガバナンスに関する対話を行うための、最低限信頼できる証拠セットを構成します。

変化する期待

OSPOがセキュリティ、AIインフラストラクチャ、コミュニティ コラボレーション、サプライヤーとのガバナンスに深く関わるようになるにつれ、経営陣の期待も変化しています。経営陣はもはや、OSPOが単にオープンソースの社内導入を指導し、ライセンス コンプライアンス チケットを処理するだけの役割を期待していません。経営陣は、OSPOが企業の複雑性を管理する上で役立つことを期待しています。したがって、狭い範囲の活動数にとらわれたままのOSPO価値測定モデルは、すでに時代遅れと言えるでしょう。

こうした状況の変化は、OSPO（組織的安全計画）の重要性を高めると同時に、その価値や影響を適切に測定できないことによるコストも増加させます。なぜなら、経営陣の認識の誤りが、投資不足、範囲の誤ったガバナンス、そして盲点へとより直接的に繋がるからです。

AI生成コード：ガバナンスの複雑さが増す

AI支援開発ツールは、コードが企業に取り込まれる方法を変えつつあり、それらが提起するガバナンス上の問題は、既存の取り込みワークフローにうまく収まりません。TODO GroupとLinux Foundationが2025年に実施した調査によると、OSPOの79%が、生成型AIリスクの管理において効果的であると自己評価しており、これは2024年の65%から上昇しています。これは真の進歩を示していますが、読者はこれらの数値が自己申告によるものであり、OSPOのAIリスク管理に関する外部ベンチマークはまだ公表されていないことに留意する必要があります。

AI生成コードに関する主な懸念事項は、出所とライセンス汚染です。公開コード リポジトリで学習された大規模な言語モデルは、ライセンス条項が不明確または議論の余地のあるパターン、慣用表現、または断片を再現する可能性があります。AI生成コードの法的地位は管轄区域によって異なり、未だに確定していません。OSPOにとって、このような状況は新たなコンプライアンス リスクを生み出し、現在のほとんどのSCAツールではこれを確実に検出できません。

測定における実際的な意味合いとしては、レジリエンスと先見性の両方の側面において、AIコードガバナンスに特化した指標を含めるべきである。具体的には、組織が製品におけるAI生成コードを管理するポリシーを持っているか、開発者がそのポリシーについてトレーニングを受けているか、そしてAI支援による貢献が本番コードベースに組み込まれる前にレビュー経路が存在するか、といった点です。

測定のための設計原則

有用なOSPO測定ポートフォリオは、短期的な経済状況、構造的な備え、先見的な探知、そして長期的なエコシステムの位置づけといった、いずれか一つに過度に集中するのではなく、これらの要素を網羅する必要があります。ただし、これらの側面を独立したカテゴリとして、あるいは固定された指標リストとして扱うべきではありません。OSPO指標ワーキンググループが採用している目標・質問・指標のアプローチに従い、OSPOはまず支援したい組織目標を明確にし、回答する必要のある経営上および運用上の質問を特定し、意思決定のための有意義な証拠を提供する指標を選択することが推奨されます。

OSPO測定の核心的な目的は、その影響を伝えることです。つまり、オープンソース活動が組織にもたらす経済的、運用面、戦略的、そしてエコシステム的な価値を伝えることです。これには、エンジニアリング、製品開発、法務、セキュリティ、調達、コミュニティ、経営陣など、さまざまなチーム間でその影響を伝えることが含まれます。

この意味で、本レポートで提案する4つの側面は、OSPOの影響を伝えるための補完的な視点として理解できます。これは、リーダーがサイバーセキュリティ、プラットフォームの信頼性、アーキテクチャの健全性、製品の品質を評価する方法と概念的に類似しています。この設計原則が、本レポートで提案するフレームワークに直接つながります。

CHAOSS実践者ガイド

CHAOSS Practitioner Guide Series（CHAOSS実践ガイドシリーズ）は、オープンソース プロジェクト組織（OSPO）がオープンソースプログラムの価値を最大限に高めるための実践的なリソースを提供します。ガイドでは、組織への影響の実証、依存関係の健全性と持続可能性の評価、プロジェクトのアーカイブと廃止の管理、オープンソース資金調達イニシアチブの成果測定など、主要な分野を網羅しています。さらに、貢献者の持続可能性、コミュニティの対応力、組織の関与、セキュリティ、リーダーシップの多様性といった側面から、オープンソース プロジェクトの改善を支援するガイダンスも提供しています。

4次元OSPO価値フレームワーク

OSPOの影響を捉えることができる単一の指標は存在しません。効果的なOSPO価値測定には、体系化された証拠のポートフォリオが必要です。図1で提案され、表1で詳細が示されているOSPO価値フレームワークは、OSPO価値を4つの次元に分類しています。各次元は、OSPO活動とビジネス成果を結びつける因果関係によって定義されます。

- **ROIとコスト削減**：重複作業や手戻りを削減することで、エンジニアリング効率が向上し、開発および保守コストが削減されます。
- **レジリエンス**：依存関係の可視化とガバナンスにより、問題の検出と修復の速度が向上し、インシデントの発生頻度と期間が短縮され、サービスの継続性が向上します。
- **リスク予測**：依存関係を継続的に監視することで、脆弱性を早期に認識できるようになり、リスクにさらされる期間が短縮され、セキュリティ インシデントの発生確率と影響が軽減されます。
- **戦略的な影響力**：積極的な上流工程への参加は、プロジェクトの方向性に対する影響力を高め、必要な能力の迅速な導入を可能にし、内部開発の必要性を低減します。

帰属に関する議論を避けるためには、価値判断の論理を明確に述べることが有効である。

OSPOメカニズム
（ポリシーと意思決定権、標準化されたプロセス、ワークフローとツール、貢献ガバナンス、サプライヤーの期待、エスカレーション設計、および内部支援）

企業能力の強化
（可視性、標準化、対応速度、部門横断的な連携）

ひいては、以下のような成果につながる
（回避可能なコストの削減、継続性の向上、早期介入、そして生態系の主体性の向上）

したがって、このスコアカードは、これらの能力開発経路が強化されている証拠として捉えるべきであり、OSPOだけがすべての下流成果を所有しているという主張として捉えるべきではありません。経路の有効性を検証する有効な方法として、OSPOの成熟度が上昇しているにもかかわらず、当該次元の成果指標が2期連続で横ばい状態にある場合、経路はまだ設計どおりに機能していないため、OSPOは成果物やプロセスが実際に意思決定に活用されているかどうかを調査する必要があります。

図 1
OSPO価値フレームワーク

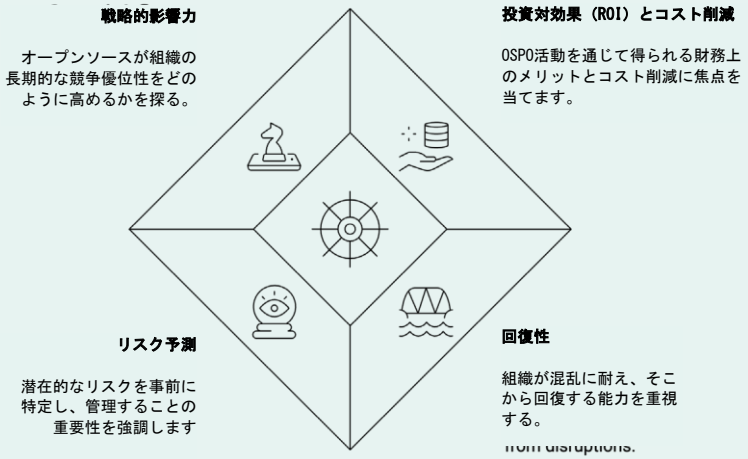


表 1

OSPO価値フレームワークにおける各次元の主な特徴

価値次元	この次元が扱う核心的な問い	主な対象者	測定期間	典型的なエビデンス	付録の章
投資対効果とコスト回避	OSPOがなかったら、私たちはどれくらいの費用を費やすことになるだろうか？	最高財務責任者（CFO）、財務担当、最高執行責任者（COO）	月次／四半期	コスト削減予測、サイクルタイム改善、外部支出の回避	A.2
レジリエンス	サプライ チェーンやガバナンスの混乱に耐える準備は、どの程度整っているのだろうか？	最高技術責任者（CTO）、最高情報セキュリティ責任者（CISO）、エンジニアリング部門リーダー	四半期／年次	カバレッジ、依存関係の可視化、準備状況指標	A.3
リスク予測	統治能力を維持するために、我々はどのような重要な問題を早期に発見できたのか？	法務、セキュリティ、取締役会、リスク委員会	四半期／年次	早期警告、リリース前介入、エスカレーションの回避	A.4
戦略的影響力	オープンソースは、組織が製品目標を達成する上でどのように役立つのか、そしてより広範には、組織の使命とビジョンの実現をどのように支援するのか？ オープンソースは、長期的な影響力と選択肢をどのように強化するのか？	最高経営責任者（CEO）、戦略、製品開発リーダー	年次／複数年	エコシステムにおける役割、標準化への参加、ロードマップとの整合性、依存関係の活用	A.5

OSPO価値フレームワーク全体の説明責任

このフレームワークを適用する前に、組織はOSPOが所有するものと、OSPOが実現するものを明確に区別する必要があります。この2つを混同することは、スコアカードの過大評価や部門間の摩擦の一般的な原因となります。

OSPOは、測定システムの設計、ガバナンス メカニズム（ポリシー、標準ワークフロー、意思決定権限、エスカレーション パス、再利用可能な成果物）、および成果を実現するための部門横断的な調整について責任を負います。ただし、これらのメカニズムが関わるすべての成果について責任を負うわけではありません。

法務部は、法的解釈および法的リスクの受容に関する決定について責任を負います。OSPOは標準的な受付経路を提供し、弁護士を必要とする反復的な案件の数を削減します。残りの決定については、法務部が責任を負います。

セキュリティ部門は、脆弱性への対応とセキュリティ リスクへの対応に責任を負います。OSPOは、依存関係の透明性、上流の状況把握、および一貫性のあるサプライ チェーン ガバナンス インターフェースを実現し、セキュリティ部門が対応を担います。

エンジニアリング、プロダクト、アーキテクチャの各チームは、実装の選択と運用実行に責任を負います。OSPOは、一貫性のある選択肢、エスカレーション経路、および再利用可能な成果物を可能にし、これらのチームがビルドとリリースの決定権を持ちます。

調達部門とサプライヤーは、該当する場合、商取引条件およびサプライヤーのコンプライアンスについて責任を負います。OSPOはオープンソースの要件と証拠に関する期待事項を定義するのに役立ち、調達部門は契約関係を所有します。

この責任マップなしに4次元スコアカードを読むと、どちらの方向にも帰属の誤りが生じる。つまり、OSPOは過剰な功績を主張するか、あるいは自分たちには責任のない結果の責任を負わされるかのどちらかになります。

各側面は、OSPOが企業価値を実現する異なるメカニズムを捉えています：

- ROIとコスト回避は、OSPOが不要な支出、摩擦、および無駄を削減するかどうかを測定します。
- レジリエンスとは、組織がオープンソースやサプライ チェーンの混乱を吸収するための構造的な準備ができているかどうかを測定する指標です。
- リスク予測とは、組織が潜在的な問題を早期に検知し、それが深刻な事態に発展する前に対応できるかどうかを測定する指標です。
- 戦略的影響力とは、組織が、実質的に依存しているエコシステムにおいて、影響力、選択肢、そしてより意図的な地位を構築しているかどうかを測定する指標です。

例えば、レジリエンスとリスク予測は関連していますが、互換性があるわけではありません。レジリエンスとは、準備状況、つまり組織が可視性、統制、成果物、対応策をどの程度整えているかということです。一方、リスク予測とは、早期発見と先を見越した介入、つまり組織がまだ対処可能な段階で発生する問題をどの程度把握できるかということです。一方の側面は、企業が混乱に耐えられるように構築されているかどうかを問い、もう一方の側面は、混乱を早期に認識して結果を変えることができるかどうかを問います。

AI生生成コードに関する注記

2025年以降、リスク予測には、標準的なライセンスおよび脆弱性検出とは別の、独立したシグナル カテゴリとして、AI生成コード ガバナンスの監視を含めるべきです。標準的なSCAツールはこの種の脆弱性に対応するように設計されていないため、検出方法も異なります。

具体的な例：単一の出来事から4つの次元すべてを読み取る

上流プロジェクトの健全性を監視するOSPOが、収益に直結する3つの製品で使用されている暗号ライブラリの唯一のメンテナーが、例えば47日間、プル リクエストのマージや問題への対応を行っていないことを検出しました。その一方で、未解決のプル リクエストや未解決の問題が1日に数件ずつ蓄積されています。このライブラリには共同メンテナーが登録されておらず、後継者に関する文書も存在しません。

これを4つの次元を通して読み解くと：

- **リスク予測の観点から見ると、これは早期警告です。**組織は、ガバナンスの不安定性がサポートやセキュリティ上のインシデントに発展する前にそれを検知しました。予測指標では、最初の兆候から47日間の検出遅延で特定された、リスクの高い上流の問題が1件記録されています。
- **レジリエンスの観点から見ると、状況にはギャップが存在します。**依存関係には担当者が割り当てられておらず、緩和策も文書化されておらず、フォークや代替案も存在しません。レジリエンス指標は、エスカレーション パスが指定されていない重大な依存関係を反映しており、これはまさにカバレッジ指標が明らかにするべき点です。
- **ROIの観点から、OSPOが今すぐ介入すれば、コストは測定可能です。**代替ライブラリの特定、プロジェクト コミュニティとの連携、共同保守への貢献開始に必要なエンジニアリング時間です。例として、シニア エンジニアの作業時間で40～80時間程度が挙げられます。対照的なシナリオは、ライブラリが放棄または侵害された後に時間的制約の中で緊急移行を行う場合で、エンジニアリング、セキュリティ レビュー、リリース再認定にかかるコストは通常4～10倍、さらにリリースが遅れた場合は遅延コストも発生します。回避された中断の価値は、これら2つのシナリオの差額から、介入なしでライブラリが実際に失敗する確率を差し引いたものです。ここに示した数値はあくまでも例示であり、業界ベンチマークではありません。組織は、これらの数値を自社のインシデント記録、またはCHAOSSやOpenSSFクリティカル スコアなどで追跡される上流の保守担当者の健全性シグナルに基づいて設定する必要があります。失敗確率が20～30%と低い場合でも、早期介入の期待値は通常、そのコストを何倍も上回ります。OSPOが文書化すべきなのは、行動だけでなく、その論理もです。
- **戦略的な影響力の下では、これはチャンスです。**組織が既に依存しているライブラリにおいて共同保守者の役割を担うだけの技術力を持っている場合、受動的な依存状態を依存力の活用へと転換できます。これは明確な道筋を持つ戦略的な成果です。

この単一の出来事は、どの側面においてもスコアカードの上位を占めるものではありません。しかし、4つの側面すべてを通してこの出来事を読み解くと、このフレームワークがチェックリストではなく、診断システムとして機能していることがわかります。

次元１：投資対効果（ROI）とコスト回避

このセクションでは、ROIとコスト回避を経済的な観点から捉えます。オープンソース ガバナンスの改善による成果としては、回避可能な支出の削減、外部依存度の低下、後期段階での混乱の減少、そしてチーム間で相乗効果を生む効率性の向上などが挙げられます。こうした価値の多くは予防的または分散的なものであることから、不正確な精度ではなく、明確な前提に基づいた規律ある見積もりによって測定されるべきです。特にこの点において、OSPOが直接生み出す価値と、エンジニアリング、法務、セキュリティ、調達といった各部門でOSPOが実現する価値を区別して報告することで、信頼性が向上します。

この次元の重要性

多くの経営幹部にとって、最初の疑問は経済的な側面です。組織がOSPOに投資した場合、どのような見返りが得られるのか、という点です。この疑問はもっともですが、往々にして視野が狭すぎます。OSPOが直接的かつ独立した形で収益を生み出すことは稀です。その財務的貢献は、コスト削減、効率化、無駄の削減といった形でより顕著に現れます。これは、企業環境において価値を表現する最も説得力のある方法の一つです。財務責任者は、支出の削減、外部依存の低減、プロセス効率の向上、納品遅延の減少といった指標に基づいて、プログラムを評価します。

この次元に属するものは何ですか？

ROIとコスト回避は、より高価な代替手段を適切に置き換えること、繰り返し発生するオープンソース問題に対する外部の法的レビューへの依存度を低減すること、問題が早期に発見されることで修復コストを削減すること、最終段階での予期せぬ事態によるリリースの中断を減らすこと、チームが標準的なガイダンスと承認された手順に従うことで重複作業を減らすことなど、経済的な成果を捉えるべきです。また、個別に見れば小さな効果であっても、全体として見れば大きな意味を持つ効率性の向上策も含めるべきです。

例えば、より迅速な情報収集ワークフロー、より明確な意思決定権限、チーム間での重複作業を削減する再利用可能な成果物などが挙げられます。

投資対効果（ROI）とコスト削減効果を測定する方法は？

OSPO（オンライン販売プラットフォーム）にとって最も効果的な財務報告は、不必要な精密さではなく、規律ある概算に基づいています。経営陣は、前提条件が明確で、方法論が安定しており、主張が控えめであれば、概算を概算として受け入れる傾向があります。

見積もりの信頼性を維持する実践的な方法は、基準値と明確な反事実シナリオに基づいて見積りを確定することです。組織は、過去の是正措置やリリース遅延の記録、サンプル製品、外部顧問弁護士への依頼パターン、繰り返し発生するガバナンス業務に費やした時間分析などを活用して、現在通常支払っている金額を把握できます。次に、ガバナンスのうち、制御可能なものと構造的なものを区別します。このアプローチにより、ROIの主張が明確になり、原因究明に関する議論を減らすことができます。

財務部門が回避コストの見積もりを検証しない場合は、財務上の主張としてではなく、透明性のある前提条件に基づいた運用上の指標として報告してください。このアプローチにより、スコアカードの信頼性を維持しつつ、優先順位付けの意思決定を支援することができます。

OSPOによって生み出された価値とOSPOによって実現された価値の違い

考慮すべき重要な点は、OSPOが直接生み出す価値と、組織全体でOSPOが実現する価値を区別することです。OSPOが生み出す価値は、標準化された受付経路、再利用可能なコンプライアンス成果物パ

イプライン、あるいは繰り返し行われるアドホック レビューに代わるガバナンス決定など、OSPOがエンドツーエンドで責任を負う成果に限定するのが最適です。OSPOが実現する価値とは、エンジニアリング、法務、セキュリティ、調達、または製品チームによって提供される成果を指し、OSPOの仕組みによって、より迅速、安全、または低コストで成果が得られる場合を指します。

例えば、OSPOは、ライセンス オプションを早期に明確化することでリリース遅延を防ぐことができますが、是正措置の実行は製品チームとリリース オーナーが行います。同様に、OSPOはテンプレートとエスカレーション ルートを作成することで外部弁護士費用を削減できますが、費用削減の実現は法務部門が行います。これらを有効活用された価値として扱うことで、貢献度の明確化が図られ、信頼の向上につながります。

よくある間違い

組織はこの側面において、以下の4つの繰り返し発生する誤りを犯しがちです。既に他の場所で認識されている節約効果を二重計上すること、すべてのオープンソースの利点をOSPOによって生み出された利点として扱うこと、明確な前提条件なしに楽観的な見積もりを提示すること、そして代替の議論を行う際に隠れたサポートやメンテナンスのコストを無視することです。

関連する安全策として、会計処理方法の変更や業務の他チームへの移管だけで改善するような指標は避けるべきです。節約効果が本物であれば、前提条件、費用源、および費用負担者は、時間の経過とともに明確かつ安定した状態を維持すべきです。

次元2：レジリエンス

このセクションでは、レジリエンスを、組織がオープンソースやソフトウェア サプライチェーンの混乱を、場当たり的な対応や後手に回ることなく吸収できる準備態勢と定義します。問題が発生するかどうかではなく、依存関係の可視化、所有権、標準化された成果物、エスカレーション パス、意思決定権といった構造的な準備態勢に焦点を当てています。したがって、レジリエンスはリスク予測とは異なります。レジリエンスは準備態勢を測定するのに対し、リスク予測は早期警戒とタイムリーな介入を測定するものです。

ガバナンスから継続性へ

ROIが、OSPOが財務部門にとって重要な理由を説明するなら、レジリエンスはOSPOがエンジニアリング部門やセキュリティ部門のリーダーシップにとって重要な理由を説明します。

現代のソフトウェア サプライチェーンは、過小評価されがちなほど脆弱です：

- 重要なパッケージは、少人数のチームによって保守される場合があります。
- 重要な上流プロジェクト間で、ガバナンスにばらつきがある可能性があります。
- 推移的依存関係はリスクを隠蔽する可能性があります。
- ビルド システムは、目に見えない複雑さを蓄積する可能性があります。
- サプライヤーの可視性が不完全な場合があります。

こうした状況下では、レジリエンスは戦略的な特性となります。OSPOは、組織がこの複雑さを可視化、構造化、管理できるようにすることで、レジリエンスの向上に貢献します。依存関係の可視性を高め、成果物の品質を強化し、一貫性のある制御パスをサポートし、上流工程やサプライチェーンの状況が悪化した場合に企業が取るべき行動を明確にします。

この次元に属するものは何ですか？

レジリエンスとは、組織の準備態勢として理解されるべきものです。これには、依存関係の可視化、SBOM（ソフトウェア部品表）の網羅性、重要な依存関係クラスターの所有権、標準アーティファクトの生成、ライセンスや出所に関する懸念事項へのエスカレーションパス、およびサプライヤーの問題に対するパッチ適用、貢献、置換、フォーク、エスカレーションに関する意思決定の準備状況が含まれます。

SBOMカバレッジを指標として用いるには、まず慎重な定義が必要です。実際には、以下の3つの条件が重要になります。

1. **フォーマット**：SPDXおよびCycloneDXで生成されたSBOMは、すべての下流のコンシューマー間で互換性があるわけではないため、組織は、どのフォーマットをどのコンシューマー向けに生成するか、またそれらのコンシューマーが実際にその出力を取り込めるかどうかを指定する必要があります。
2. **鮮度**：リリース時に生成されたSBOMは、その時点では正確です。製品の運用期間中に基礎となる依存関係が変化し、SBOMが更新されない場合、高いカバレッジ スコアと運用上の盲点が共存する可能性があります。
3. **消費**：調達決定、脆弱性対応ワークフロー、またはサプライヤーとの会話において参照されていないSBOMは、存在するものの、機能ではない。

したがって、カバレッジ指標は、簡単な運用テストと組み合わせるべきです。つまり、直近の四半期で、SBOMが実際に意思決定を行う、または意思決定を加速するために何回使用されたか、ということです。

このテストを運用可能にするために、組織はSBOMを参照する決定事項について、単一の追跡ポイントを指定する必要があります。これは、リリースチェックリストの項目、脆弱性対応チケットのタグ、

または調達承認記録の行など、いずれでも構いません。この質問では、SBOMが参照されるたびに、それがどのような決定に役立ったかを記録する責任を負う人物が必要であるとされています。年間12件の記録があれば、運用に使用されているという確かな証拠となります。記録がゼロであれば、網羅率に関係なく、単なる記録の寄せ集めに過ぎないという証拠となります。

したがって、レジリエンスとは、ストレスが発生した際にリスクをより適切に管理できる構造が存在することを意味します。レジリエンスの指標は通常、遅行指標ではなく、先行指標となります。有用な指標としては、最新のSBOM（ソフトウェア部品表）を持つ製品の割合、主要な依存関係が特定され、担当者が割り当てられている重要な製品の割合、関連する上流の問題を関係者が認識するまでの時間、標準準拠アーティファクトでカバーされているリリースの割合、および明確な緩和策が設定されている高リスク依存関係の割合などが挙げられます。

レジリエンスをどのように測定するか？

過信を防ぐためには、これらの指標をシステム優先の視点から解釈する必要があります。つまり、安全性、収益、およびリリースに不可欠な製品を最優先し、スコープを明確にする必要があります。ロングテール全体にわたって高いカバレッジがあっても、最も重要なシステムに深刻なギャップが存在する可能性があるため、経営陣への報告ではスコープを可視化する必要があります。

安全策として、成果物が最新のものであり、意思決定に活用され、所有権やエスカレーション経路と結びついている場合を除き、カバレッジの数値が高いことを準備完了の証明とみなすべきではありません。そうでない場合、その指標は運用能力指標ではなく、コンプライアンス上の成果物になってしまう可能性があります。

レジリエンスはしばしば過小評価される

強固なオープンソース体制は、依存関係のリスクを完全に排除するものではありません。しかし、組織が予期せぬ事態に直面したり、それによって麻痺状態に陥ったり、高額な最終段階での意思決定を強いられたりする可能性を低減します。

レジリエンスは、失敗した時に初めてその真価が明らかになるため、投資が不足しがちです。準備作業が適切に行われていれば、劇的な事態は発生しません。リリースは計画通りに進み、問題は早期に解決されます。こうした成功は、通常の業務運営のように見えます。だからこそ、レジリエンス指標が重要なのです。これらの指標は、混乱によって高額なテストを強いられる前に、リーダーに準備状況の証拠を提供します。

次元3：リスク予測

このセクションでは、リスク予測とは、組織がオープンソースに関する新たな問題を早期に検知し、インシデント、リリースの中断、ライセンス問題、またはエスカレーションに発展する前に、結果を変える能力のことであると説明します。準備態勢を測定するレジリエンスとは異なり、予測は早期警告とタイムリーな介入を測定します。これは、先行指標と、何が検知され、どのような決定が変更され、何が回避された可能性が高いかを示す、簡潔で体系的なニアミス事例集を組み合わせることで最もよく証明されます。

OSPOの価値の一部は、レジリエンスだけでは完全に捉えきれない。SPOは、リリース前にライセンスの不適合を特定したり、上流プロジェクトのガバナンスが弱体化している兆候を認識したり、ポリシー上の問題が深刻化する前に表面化させたり、是正措置がまだ実行可能な段階でプロセスの逸脱パターンを検出したりするなど、早期警戒メカニズムとして頻繁に機能します。この機能は、単なるリスク管理というよりも、リスク予測と表現する方が適切です。既知のリスクカテゴリに対処することと、結果を変えるのに十分なほど早期に微弱な兆候を認識することの両方が重要になります。

この次元に属するものは何ですか？

リスク予測には、リリース前に問題のあるライセンスや未承認の条項を検出すること、オープンソースの使用に関連する規制やポリシーの変更を早期に特定すること、将来のサポートやセキュリティの問題を引き起こす可能性のある上流の不安定性を認識すること、承認された経路を迂回するチームを検出すること、および出所やサプライチェーンに関する懸念がインシデントになる前にエスカレーションすることが含まれます。

実際には、将来予測シグナルは通常、上流のセキュリティ勧告や脆弱性フィード、SBOMや依存関係の差分監視、メンテナーやプロジェクトの健全性シグナル、ポリシーや規制の追跡、サプライヤーの開示、内部パターンなど、複数のソースから得られます。したがって、成熟した将来予測とは、発見された問題の数だけでなく、シグナルチャネルの網羅性も重要です。この文脈において、CHAOSS OSPO WGの一環として、主にGary White氏（Verizon OSPOの主席エンジニア）によって開発された「CHAOSS Practitioner Guide: Assessing Viability」に注目する価値があります。このガイドは、主にOSPOや、利用しているオープンソース ソフトウェアに関連する実現可能性とリスクを理解する必要のある組織内の他のチームを対象としています。

リスク予測能力をどのように測定するか？

予防的価値は本質的に測定が難しい。OSPOが介入しなかった場合に何が起こったかを確実に証明することはほとんど不可能です。しかし、だからといって測定が難しくなるわけではありません。不可能だ。つまり、証拠モデルは、訴因と判決、そして短い説明文を組み合わせる必要があるということです。

有用な指標としては、リリース前に特定された高リスク問題の数、それらの問題の深刻度構成、後期段階での発見の傾向、正式なエスカレーション前に方向転換された問題の数、外部の変化に対応して発行されたポリシー勧告の数、および問題の検出から決定までの時間などが挙げられます。

よくある解釈の誤りは、発見された問題の数が多いことをパフォーマンスの低下と捉えることです。将来を見据えると、短期的な増加は、検出能力の向上とより健全な情報開示を示している可能性があります。より有意義な経営判断の指標としては、重症度構成、後期段階の発見傾向、意思決定までの時間などが挙げられます。

ニアミスは、以下の3つの条件すべてが満たされた場合にのみ「検証済み」となります。第一に、問題が阻止されなかった場合、リリース停止、セキュリティ侵害、ライセンス違反、または規制上の指摘など、測定可能な下流への影響が生じていたであろうこと。第二に、阻止が、担当者名、日付、および下された決定とともに文書化されていること。

第三に、反事実的影響が、断定的な仮定ではなく、明示された仮定に基づいて推定されていること。これら3つの条件のいずれかを満たさない件数は、有用な運用テレメトリではありますが、経営幹部のスコアカードに検証済みのニアミスとして報告すべきではありません。

予測 vs. レジリエンス

レジリエンスとリスク予測の違いは、特筆に値します。レジリエンスとは、企業がオープンソースによるショックに対して構造的に備えているかどうかを問うものです。リスク予測とは、企業が潜在的な問題を早期に察知し、ショックが深刻化する前に介入できるかどうかを問うものである。一方は準備態勢を測るものであり、もう一方は先を見越した検知と行動を測るものです。

レジリエンスとは組織が混乱に耐える能力であるとすれば、リスク予測とは組織が、混乱がまだ制御可能な段階でそれを察知する能力です。

次元4：戦略的影響力

このセクションでは、閃絡的影響力を、組織がオープンソースへの受動的な依存から、主体性、影響力、および技術的選択肢を高める意図的なエコシステムへの関与へと移行する際に生み出される長期的な価値と定義します。この価値は取引的なものではなく方向性を示すものであることが多いため、具体的な関与の証拠（代表性、連携、協力）と、年間および複数年にわたる簡潔な経営幹部による説明を組み合わせることで、最も適切に評価できます。

最も成熟したOSPOは、リスクの軽減やコンプライアンスの支援にとどまらず、組織が依存するエコシステムへの参加方法を形作ります。標準規格、貢献の優先順位、依存戦略、サプライヤーの期待、そして新興技術に対する組織内の姿勢に影響を与え、企業が受動的な消費から意図的な参加へと移行するのを支援します。

これは重要な点です。なぜなら、オープンソースは調達モデルであり、戦略的な環境でもあるからです。そこでは、可視性、貢献、ガバナンスへの参加が長期的な影響力に影響を与えます。OSPOは、単にエコシステムを利用するだけでなく、企業が将来に影響を与えるエコシステムを形成するのを支援することで、戦略的に価値を持つようになります。

3つの戦略的メカニズム

戦略的な影響力は、抽象的な思想的リーダーシップの主張ではなく、具体的なビジネス メカニズムに基づいているべきです。
特に重要なメカニズムが3つあります。

1. **依存関係の活用**：組織は、重要な依存関係の背後にあるプロジェクト、コミュニティ、ガバナンス組織に単に晒されるのではなく、有意義に関与することで、より大きな主体性を発揮できます。
2. **技術の選択肢の豊富さ**：オープンソースに対する姿勢を強化することで、組織はベンダーロックインを減らし、より高い自信を持って技術を採用、開発、代替、または撤退する能力を向上させることができます。
3. **組織内での地位**：関連する財団、標準化団体、ワーキンググループに参加することで、企業は将来の技術的およびガバナンス上の意思決定が行われる場に席を確保できます。

受動的な依存による戦略的なコストは、主体性の低下である。組織は、他所で下される技術的およびガバナンス上の決定に、それらを形成する条件に対する十分な影響力を持たずに、より脆弱な立場に置かれることになります。

実践における戦略的影響力

実際には、戦略的な影響力には、関連する財団や運営グループへの参加、製品ロードマップに沿った貢献戦略、エコシステム情報やコラボレーションチャネルへのアクセス向上、社内能力の強化によるベンダーロックインの軽減、上級エンジニアの間での雇用主としての信頼性の向上、オープンエコシステムで成熟した技術の採用までの迅速な道筋などが含まれます。

戦略的な影響力は、OSPO、製品戦略、アーキテクチャ、調達、および経営陣間の内部的な連携にも左右される。外部の参加だけでは、持続的な影響力を生み出すことはほとんどありません。

なぜこの側面は定量化が難しいのでしょうか？

戦略的影響力は通常、取引的というよりは方向性を示すものです。より長期的な視点と、代表性、ロードマップとの整合性、目に見えるエコシステムへの参加、依存関係の活用、そして特定の立場がなぜ重要だったのかを説明する簡潔なリーダーシップの物語といった、多様な証拠を通して評価するのが適切です。ここで適切な基準は、

規律ある謙虚さです。説明可能な影響力については具体的に述べ、誇張した主張は避けましょう。エコシステムへの関与を、具体的な組織成果と結びつけることが重要です。

この側面を証拠に基づいたものにするためには、組織は参加ではなく影響力を主張する前に、3段階のテストを適用すべきです。

1. **ティア1は存在**：組織が会員資格を有し、会議に出席します。また、時折、内部の優先事項とは無関係に貢献を行います。
2. **ティア2はエンゲージメント**：組織は、プロジェクトに積極的に貢献するメンバーがおり、彼らの作業は製品またはプラットフォームのロードマップと関連付けられており、明確な責任者が設定された社内スポンサーシップが存在します。
3. **ティア3は影響力**：組織は、自らの参加によって技術的な決定、ガバナンスの結果、または基準が変更され、それが下流のコストやリスクに影響を与えた具体的な成果を指摘することができます。

以下のうち少なくとも1つは文書化可能である必要があります。承認され、将来の保守負担を軽減した設計提案、重要な依存関係が動作する条件を変更したガバナンスの役割、組織が策定し、その製品に適用される標準規格、または組織のプラットフォーム上の利益に資するプロジェクト ロードマップの変更です。

報告基準は単純です。もしその組織の参加を完全に除外した場合、エコシステムの成果は、実質的に同じだったでしょうか？もしそうであれば、その組織の存在を報告します。正直に言って「おそらくそうではない」という場合は、具体的な結果を添えて影響として報告することになります。戦略影響力は、インフレ影響を最も受けやすい要素であり、ここで一つでも過剰な主張をすれば、評価表全体の信頼性を損なうことになります。

ティア3の主張については、以下のいずれかの証拠によって裏付けられる必要があります。組織外の指定メンテナーまたはTSCメンバーによる貢献の重要性の確認、公に検証可能な文書化されたプロジェクト記録（承認された提案、統合された設計文書、公開された標準テキスト）、または関連する財団もしくはワーキング グループによる正式な承認。内部の説明だけではティア3の主張には不十分であり、外部の証拠が得られるまではティア2の関与として扱われるべきです。

安全策として、成果への道筋とそれがビジネスにとってなぜ重要だったのかを明確に説明できない限り、カウント（コミット数、メンバーシップ数、参加した会議数、カンファレンスでの発表数）を戦略的影響力の証拠として扱うことは避けることを強くお勧めします。

信頼性の高いOSPO価値測定システム構築のための原則

指標を定義する前に、組織はいくつかの設計原則について合意しておくべきです。

1. **活動だけでなく成果も測定する**：完了したレビュー、実施された研修、スキャンされたリポジトリ、公開されたポリシーなどは、いずれも有用な運用指標となり得ます。しかし、これらは企業価値の証拠ではありません。これらは主要な指標ではなく、補助的な指標として扱うべきです。
2. **少数の安定した指標を優先する**：公開可能なスコアカードは読みやすいものでなければなりません。経営陣によるレビューには、通常、各次元につき2〜4個の指標で十分です。目標は意思決定支援であり、指標の多さではありません。
3. **定量的証拠と記述的証拠を組み合わせる**：指標に簡潔な解説文を添えることで、OSPOの価値がより明確になります。リスク予測や戦略的影響力といった分野では、記述的要素は弱点ではなく、証拠モデルの一部となります。
4. **前提条件を明確にする**：回避できる混乱の程度を推定する場合、その前提条件を文書化する必要があります。透明性のある推定は信頼を築き、隠蔽された推定は信頼を損ないます。
5. **実現価値と所有価値を区別する**：信頼できるスコアカードでは、OSPOがオープンソースに関連するすべての価値を直接「創造」しているかのように示唆することは避けるべきです。ほとんどの組織では、OSPOは、企業がオープンソースを管理、採用、貢献、リスク軽減する方法を改善することで価値を実現します。測定は、この実現的な役割を反映するべきです。成果指標が改善した場合（MTTRの低下、監査準備時間の短縮、後期段階での発見の減少など）、同じ変化を引き起こした可能性のある代替原因を少なくとも1つ挙げ（同時並行のツール変更、セキュリティチームの取り組み、ベンダーSLAの変更など）、OSPOの貢献がそれらの代替原因からどのように分離されているかを明記してください。
6. **情報開示を罰する指標を避ける**：チームが、問題点が表面化すると、パフォーマンス指標が悪化し、システムは改善ではなく盲目状態を生み出すことになります。OSPOの措置は、問題の早期発見を奨励するべきであり、問題を隠蔽するインセンティブを生み出すべきではありません。
7. **成熟度を考慮した設計**：信頼性の高いデータを収集し、時間とともに改善していくことです。優れた測定プログラムは反復的なプロセスを経て構築されます。
8. **フレームワークの限界を述べる**：このフレームワークはOSPOのすべての価値を収益化できるとは主張しません。完全な帰属を保証するものではありません。詳細なエンジニアリング、セキュリティ、または法的報告に取って代わるものでもありません。また、経営陣の判断を排除するものでもありません。その目的はより限定的で実践的なものであり、オープンソースのガバナンスが企業の成果にどのような影響を与えるかを構造的に評価する方法を提供することです。
9. **評価基準の連続性を保護する**：意図的に、かつ稀に変更するべきです。指標のロジック、分母、またはソースの基準が変更された場合は、その変更内容を文書化し、バージョン管理を可視化する必要があります。そうしないと、測定システムが変更されたというだけの理由で、ダッシュボードが改善されたように見えてしまうリスクがあります。OSPOの組織範囲が、再編、拡大、または他部門との合併などによって大幅に変更される場合、スコアカードには、変更内容と過去のデータとの比較可能性への影響を説明するバージョン情報を含めるべきです。測定の継続性は、報告原則だけでなく、組織的意思決定における設計原則であるべきです。

経営幹部向け報告モデル

最も効果的なOSPO報告モデルは、定期的に提供されるバランスの取れたエグゼクティブ スコアカードです。このスコアカードには、4つの側面を簡潔にまとめた1ページの要約、それぞれの側面に関する少数の傾向指標、動向と影響を説明する短い解説、そしてニアミスや介入によって数値が明確になった事例に関する記述を含めるべきです。

経営層にとって有用な指標とするには、各指標にシンプルな意思決定ループを関連付ける必要があります。つまり、その指標が何を意味するのか、改善または悪化した場合にどのような対策が取れるのか、誰がその対策を担当するのか、そして効果が現れるまでの期間はどのくらいと予想されるのかを明確にするのです。このアプローチにより、スコアカードが単なる記述的な報告書になるのを防ぎ、ガバナンス ツールとして活用できるようになります。

対象者に合わせたカスタマイズ

基となるデータが同じであっても、対象となる経営幹部層によって、強調すべき点は異なります。

- **CFO/COO**：コスト削減、サイクルタイム改善、外部支出削減、リリース経済性
- **CTO/エンジニアリングリーダーシップ**：依存関係の透明性、リリース準備、貢献の活用、および運用継続性
- **CISO/リスクリーダーシップ**：リリース前の問題発見、問題認識までの時間、コントロールの網羅性、ガバナンスの質
- **CEO/戦略/取締役会**:エコシステムの活用、規制準備態勢、戦略的貢献の整合性、および長期的な能力構築

対象者に合わせた調整は、スコアカードの根底にある真実の条件ではなく、重点の置き方を変えるべきです。目的は、異なる利害関係者向けに並行した説明を用意することではなく、部門横断的な協調的な解釈を行うことです。

- **OSPO**：測定システムの設計、部門横断的な調整、および企業成果を可能にするガバナンス メカニズムに責任を負います。
- **法務**：法解釈および法的なリスク受容に関する決定（例えば、ライセンスに関する立場や例外など）について責任を負い、OSPOが標準的な手順と受付規律を提供します。
- **セキュリティ**：セキュリティリスクの姿勢とOSPOは、依存関係の透明性、上流工程の把握、および一貫性のあるサプライチェーン ガバナンス インターフェースを可能にすることで、脆弱性への対応を可能にします。
- **エンジニアリング、製品、アーキテクチャ**：実装の選択（パッチ適用、置換、フォーク、コントリビュート）と運用実行に責任を持ち、OSPOによって一貫性のあるオプション、エスカレーション経路、再利用用可能な成果物を実現します。
- **調達およびサプライヤー**：該当する場合、商取引条件およびサプライヤーのコンプライアンスに責任を負い、OSPOはオープンソースの要件および証拠の期待を定義するのに役立ちます。

サンプル スコアカード

下記の表2は、OSPO四半期スコアカードのサンプルであり、例示的な値が示されています。ステータスの閾値はディメンション レベルに設定されています。すべての値は例示です。組織は、この形式を採用する前に、自社の規模、業界、およびOSPO成熟度段階に合わせて目標を調整する必要があります。また、ここに示されている例示的な数値を採用するのではなく、測定年度の開始時に基準値を設定し、目標を設定する必要があります。

表には注目すべき点が2つあります。SBOMの網羅性とSBOMの鮮度は、それぞれ異なるものを測定しているため、別々の行になっています。組織はほぼすべての生産依存関係のSBOMを保有していても、そのほとんどが古くなっている可能性があります。どちらもEU CRAへの対応準備において重要であり、これらを1つの指標にまとめてしまうと、どの問題を解決すべきかが分かりにくくなります。同様に、検証済みのニアミス件数が3件と少なく見えますが、これは意図的なものです。3つの条件すべてを満たすニアミスのみがカウントされます。しきい値を満たさない非公式な報告を含めることで件数を水増しすると、この指標の目的が損なわれてしまいます。

表2

サンプルOSPOスコアカード

次元	指標	現在	目標	状態	傾向	所有者
投資対効果とコスト回避	内部再利用率	34%	45%		▲	エンジニアリングプラットフォーム
	ライセンス是正費用	$250,000	$150,000		►	OSPO/法務
	監査準備期間（日数）	11	5		▼	OSPO
	承認済みコンポーネントの採用率	61%	80%		▲	エンジニアリング
レジリエンス	SBOM（部品表）の網羅範囲（生産依存）	78%	95%		▲	セキュリティ/OSPO
	SBOMの鮮度（更新日：90日以内）	64%	90%		►	セキュリティ
	重大なCVEに対するパッチ適用にかかる平均時間	9 days	5 days		▼	セキュリティ
	重要な単一メンテナー依存関係	14	<5		►	OSPO

次元	指標	現在	目標	状態	傾向	所有者
リスク予測	検証済みのニアミス事例（四半期）	3	4＋		▲	OSPO
	公開前に特定されたCVE	2	4＋		▲	セキュリティ
	AIコードポリシーの適用範囲（チーム別）	55%	100%		▲	エンジニアリング
	CRA準備度スコア（自己評価）	62/100	80/100		▲	法務/OSPO
戦略的影響力	ティア1プレゼンス（戦略的プロジェクト）	8	10		▼	OSPO
	ティア2のガバナンス役職を歴任	4	6		▲	OSPO
	ティア3外部検証イベント	2	2＋		▶	OSPO
	依存度影響比	0□31	0□40		▲	エンジニアリング

Legend:

▲ 増加 ▶ 横這い▼ 減少

目標以上のパフォーマンス

目標値の20%以内の成績

四半期の業績が目標を20%以上下回る、または目立った進展が見られない

CRAへの対応準備に関する注記：

この行のスコアは自己評価であり、監査レベルの証拠としてではなく、準備状況の指標として解釈してください。外部の評価基準（例えば、将来のOpenChainガイダンスなど）が利用可能になった場合は、このスコアをその基準に合わせて、「自己評価」という表記を削除してください。

ティア1の存在に関する注記：

これはカウント指標であり、戦略的影響力の証拠としてではなく、文脈を示すものとして報告されています。影響力に関する主張は、ティア2およびティア3の行を参照してください。

OSPOの進化に伴い、測定方法も進化する

組織は、それを支える基盤が整う前に高度なスコアカードを導入しようとすべきではありません。測定の成熟度は一般的に4つの段階を経て進み、各段階には異なる報告目標と、行き過ぎのリスクがあります（表3および図2を参照）。

表3

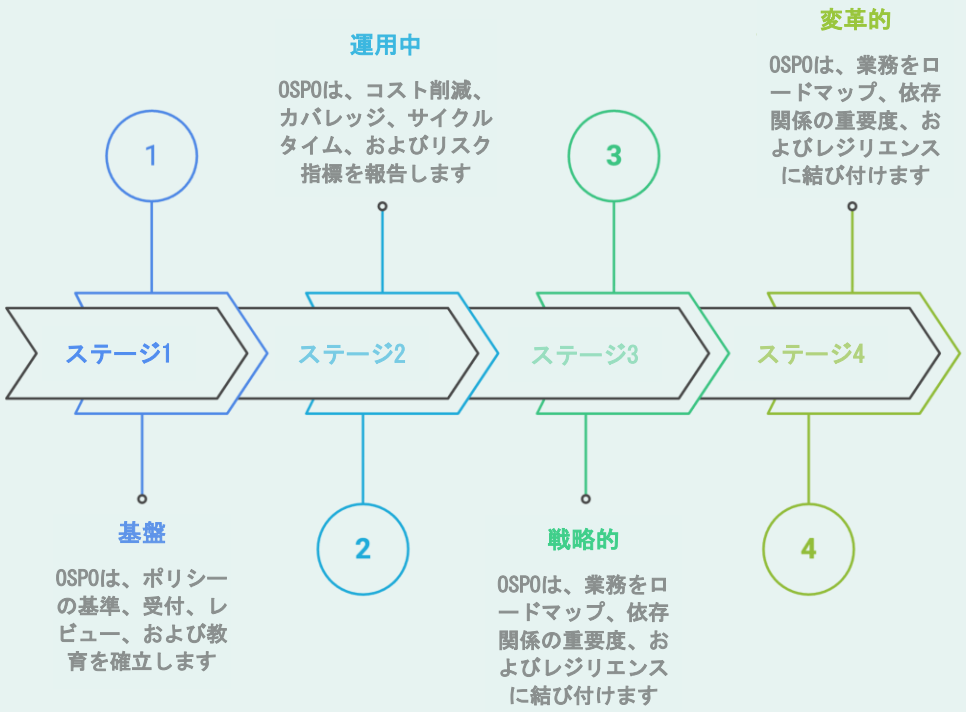
OSPOSの進化に伴う測定方法の進化

ステージ	説明	報告	目的	回避
OSPOステージ1：基礎	OSPOは、政策基準、受付プロセス、審査経路、および基礎教育を構築しています。	報告は主に活動に基づいて行われる。	可視性と一貫性	OSPO機能が安定したプロセスやデータを持つようになるまでは、完全なROI証明を要求することは避けてください。
OSPOステージ2：運用中	OSPOは、コスト回避指標、カバレッジレベル、サイクルタイム、および基本的なリスク指標を報告できるようになりました。	データ所有権がり明確になり、いくつかのダッシュボードが登場することで、レポート作成が改善される。	再現性	不安定な指標を早々に追加しすぎないようにしましょう。
OSPOステージ3：戦略的	OSPOは、その活動を製品ロードマップ、依存関係の重要度、貢献の優先順位、およびレジリエンスの成果と結びつけ始めます。	報告はより結果重視になっている。	ビジネス関連性	生態系活動と戦略的影響力を混同しないように注意します。
OSPOステージ4：変革的	OSPOは、エコシステムにおける地位、ガバナンス体制、戦略的先見性に対して測定可能な影響力を持つ、認知された企業機能として機能します。	レポート作成では、財務、業務、戦略の各視点を統合します。	エンタープライズ統合	証拠に基づかないレトリックは避けるべきです。

このモデルは測定の成熟度を説明するものであり、必ずしもガバナンスの成熟度と同じペースや順序で追跡されるとは限りません。組織によっては、洗練されたオープンソース ガバナンス、適切に設計されたポリシーとプロセス、一貫した貢献慣行、強力な上流関係を備えていても、データ収集、報告規律、部門横断的な計測に投資していないために、測定インフラストラクチャがステージ1のままになっている場合があります。その逆もまた起こり得ます。適切に計測されたダッシュボードを備えた小規模なOSPOは、数値が明確であるため、実際よりも成熟しているように見えることがあります。

図2

OSPO段階ごとの主要指標



したがって、リーダーはモデルを診断的に2つの軸に沿って活用すべきである。1つ目はガバナンス能力、すなわち基盤となる実践の成熟度である。2つ目は測定能力、すなわち組織はそれらの実践をどの程度確実に観察し報告できるかです。この2つの軸の間には不一致がよく見られるため、明確に指摘しておく必要があります。なぜなら、それぞれに異なる是正戦略が必要となるからです。

実際には、成熟度はフレームワークのすべての側面において必ずしも均一ではありません。組織はコンプライアンスの可視性やレジリエンスの指標においては比較的進んでいる一方で、戦略的影響力や将来予測の報告においては初期段階にとどまっている場合があります。したがって、このモデルの目的は、厳密に順序立てたものではなく、診断的なものです。目標はステージ4に急いで到達することではなく、理想論ではなく、組織の実際の成熟度を反映した報告モデルを構築することです。

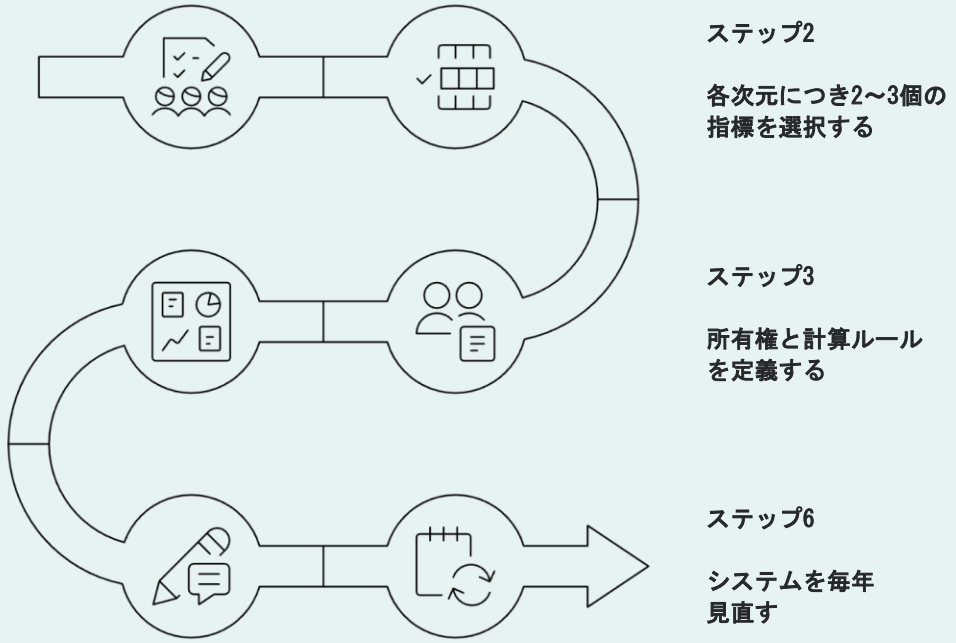
実践的な導入ロードマップ

実際の実装手順は簡単です（図3参照）：

1. **経営陣との連携**：指標を用いる際には、経営陣がどのような種類の洞察を求めているのかを理解し、望ましい洞察につながる指標の採用計画について経営陣と協議することが重要です。このプロセスは通常、継続的なフィードバック ループを伴う双方向的なものです。
2. **各次元につき2〜3個の指標を選択する**：最初は小規模なものから始める。重要で、理解しやすく、安定していて、収集可能な指標を選択します。
3. **所有権と計算ルールを定義する**：すべての指標には、所有者、計算方法、測定頻度、文書化された注意点、および特定されたソース システムまたはソース ワークフローが必要です。手動によるデータ収集や判断が伴う場合は、リーダーが指標の信頼性と限界を理解できるよう、その旨を明確にする必要があります。
4. **ダッシュボードを1〜2四半期にわたって試験運用する**：最初の報告期間は調整期間とみなします。この期間を利用して、定義の曖昧さ、データ品質の低さ、または不適切なインセンティブを生み出す指標を特定します。
5. **事例に関する記述を追加する**：パイロット運用中は、指標の持続的な変動を単なる解釈ではなく、行動を促すきっかけとして捉えましょう。指標が2期間連続で悪化した場合は、担当者、根本原因分析、および日付入りの是正措置を要求します。指標が改善した場合は、組織がそれを再現できるよう、何が変わったのかを記録します。特に将来予測や戦略的影響力においては、短い事例に関する記述は、別の数値フィールドよりも多くの価値を伝えることがよくあります。
6. システムを毎年見直す：OSPOが成熟するにつれて、評価指標も進化させるべきです。更新内容には、もはや重要ではなくなった指標の廃止や、現在の経営陣の懸念事項をより適切に反映する指標の追加などが含まれます。

図3

OSPOバリューフレームワークを導入する際の手順



経営陣の支援と3人以上のOSPOチームによる集中的な実装では、部門横断的なガバナンスの連携が既に確立されている組織では、ステップ1から3は通常4〜6週間で完了します。こうした連携関係がまだ構築中の場合は、通常クリティカルパスとなるステップ3のステークホルダーの連携に4〜8週間を追加してください。最初のパイロット四半期（ステップ4）は、定義上3か月かかります。ステップ5と6は継続中です。したがって、ステージ1からステージ2の成熟度を持つ信頼できる最初の経営幹部スコアカードは、開始から5〜7か月以内に達成できるはずです。ステージ3のレポート（成果重視、多次元）に到達するには通常より時間がかかり、部門横断的なデータ計測に依存します。データ所有権が分散している大規模組織では、期間を2倍にしてください。これらの数値は、著者がこの作業を通じて組織に助言してきた経験を反映したものであり、公表された研究のベンチマーク データではありません。最も一般的な失敗モードは技術的な困難ではなく、完璧なデータが揃うまで何も公開しないことです。たとえいくつかの指標に明確な不確実性範囲が含まれていても、試験運用期間の終わりに、ラベルを分かりやすく記載した初稿のスコアカードを公開しましょう。完璧ではないダッシュボードでも、公開すれば、公開されない完璧なダッシュボードよりも組織の信頼性が高まります。

結論：OSPOの物語を再構築する

本報告書で提示したフレームワークを導入してから3年後、2種類の組織が出現しました。1つ目の組織は、詳細なスコアカードを用いて取締役会に説明を行い、コンプライアンス違反寸前の事例と組織構造の変更を結びつけ、上流工程における影響力によってどれだけの手戻りを回避できたかを定量化できる。2つ目の組織は、依然として活動件数に頼り、人員数で正当化されることを期待しています。両者の違いは、OSPOが自らの責任を問われる前に測定インフラストラクチャを構築していたかどうかにあります。

このフレームワークにおける4つの側面は、互いに独立しているわけではありません。例えば、回復力のないROIでは、重要な依存関係が維持されなくなるまで効率的に見える組織が生まれます。リスク予測のない回復力では、対応はうまくできても、決して先を見越さない組織が生まれます。戦略的影響力のないリスク予測では、迫りくる脅威を認識しても、それに対処するためのエコシステム的な基盤が欠如した組織が生まれます。

このフレームワークの貢献は、両者を明確に区別している点にあります。レジリエンスとリスク予測は同じものではなく、これらを混同すると、見た目は似ていても、測定対象となる組織能力は全く異なる指標となります。ニアミス基準が存在するのは、遅行指標（実際のインシデント、開示された脆弱性、監査の失敗など）が、それらを引き起こした行動を変えるには遅すぎるためです。第3段階の影響テストが存在するのは、エコシステム レベルでの自己評価が信頼できないためです。

このインフラストラクチャによって可能になるのは、現在ほとんどの組織に欠けている測定と意思決定の間のフィードバック ループです。スコアカードが稼働すれば、OSPOは調達決定を上流の取引関係に、人員配置に関する議論をレジリエンスのギャップに、コンプライアンス投資を定量化されたリスク削減に結びつけることができます。これは、今日のほとんどのOSPOリーダーが行っている議論とは全く異なるものです。

提案するOSPO価値フレームワークは、あくまでも基準となる参考資料として位置づけられています。組織によって戦略的優先事項、運用モデル、オープンソースへの取り組みの成熟度は大きく異なります。そのため、このフレームワークは、個々の組織に合わせたOSPO価値ダッシュボードの設計の基盤として活用されるべきです。

実践者は、それぞれの状況に最も関連性の高い指標や次元を採用、適応、拡張することが推奨されます。実際には、効果的なOSPO価値測定は反復を通じて実現します。つまり、組織の目標、ステークホルダーの期待、そして進化するオープンソース戦略をより適切に反映させるために、指標を時間をかけて洗練させていくのです。このフレームワークを適用する組織は、ゼロから構築するよりも迅速に価値測定アプローチを構築でき、その結果はより有意義で実行可能なものとなるでしょう。

今このフレームワークを構築する組織は、OSPOの価値をより適切に測定し、オープンソースに関する組織的な障壁を減らし、より迅速な意思決定を行うことができるようになるでしょう。

付録A. OSPO評価基準カタログ

以下のカタログは、四半期ごとの経営幹部向けスコアカードに適した指標定義の例を示しています。これらはあくまで出発点であり、普遍的な処方箋ではありません。組織のガバナンスモデル、製品ポートフォリオ、およびデータの入手可能性に合わせて調整する必要があります。

A.1 評価指標設計に関する注記

各指標には以下が含まれます：

- **定義**：何が測定されているのか
- **主な対象ユーザー**：最も直接的に利用する人
- **頻度**：どのくらいの頻度でレビューすべきか
- **注意点**：解釈が誤っている可能性のある箇所
- **推奨される所有者**：測定結果を維持および追跡する担当者

さらに、各指標は、基準値、該当する場合は分母、および推奨される表示形式（例えば、件数、パーセンテージ、比率、傾向など）を明記し、解釈の一貫性を長期間維持する必要があります。また、該当する場合は、指標の範囲（例えば、最も重要な製品またはリリースラインに限定するなど）を明示的に示すことで、ポートフォリオの中で最も容易な部分のみを測定することでスコアを向上させることができないようにする必要があります。

以下の指標は業務上役立つ可能性があるが、それ自体を企業価値の主要な証拠として用いるべきではない：

- 処理したチケット数
- 実施された研修の数
- 公表された政策の数
- 処理された寄付リクエストの数
- スキャンされたリポジトリの数

これらの指標は、業務量やプロセスの成熟度を説明するのに役立つが、企業価値を測る主要な指標としてはどれも十分ではありません。

A.2 投資対効果（ROI）とコスト回避評価指標

表4

投資対効果（ROI）とコスト回避のための評価指標

評価指標	意味	顧客	頻度	注意点	所有者
推定商業再調達価格	選択したオープンソース資産が利用できない場合に購入する必要が生じる、商用ツール、プラットフォーム、またはコンポーネントの年間推定コスト。	CFO、CTO	四半期 または 年次	現実的な調達経路のない、仮説上の代替案は避けるべきです。 前提条件と信頼度を文書化します。	OSPO ＋ 財務ビジネスパートナー
外部法律レビュー費用を回避	定期的なオープンソースレビュークラスを標準化された社内処理で実施することで、外部の弁護士や臨時の専門家によるレビューが必要となる場合に比べて、推定される支出を削減できた。	CFO、法務部門責任者	四半期	回避された外部支出と延期された作業を区別します。	OSPO ＋ 法務業務
リリース遅延を防止	OSPOの早期介入によって、正式なリリースゲートやローンチ遅延が発生する前にオープンソースの問題が解決されたリリースの数。	COO、CTO、製品リーダーシップ	四半期	介入に関する文書による記録が必要です。推測に基づく遅延は考慮しないでください。	OSPO ＋ リリース管理
コンプライアンス サイクルタイムの短縮	合意された基準値と比較した、一般的なオープンソースの受け入れまたはレビューワークフローを完了するのに要する時間の中央値。	エンジニアリングリーダーシップ、COO	月次、 または、 四半期	サイクルタイムの短縮は、レビューの質を犠牲にして行うべきではありません。	OSPOオペレーションリーダー

A.3 レジリエンス評価指標

表5

レジリエンス評価

評価指標	意味	顧客	頻度	注意点	所有者
SBOM カバー率	生産予定の製品またはリリースのうち、最新の機械可読なSBOM（部品表）が入手可能なものの割合。	CTO、CISO	月次または四半期	レポートの対象範囲を明示的に指定してください。重要な本番システムのみ、またはポートフォリオ全体。同じガバナンスプログラムでも、両者で数値が大きく異なる可能性があるためです。	OSPO ＋ ツール チームを構築またはリリース
重要な依存関係の可視性	重要な依存関係が特定、分類され、所有者またはエスカレーションパスが割り当てられている重要製品の割合。	CTO、CISO	四半期	重要な依存関係の定義を文書化する必要があります。	OSPO ＋ アーキテクチャまたはサプライ チェーン ガバナンス チーム
上流の問題に対する意識を高める時が来た	関連する上流の問題が外部に公表されたり、内部で発見されたりしてから、責任ある利害関係者が組織内でその問題を認識するまでの経過時間の中央値。	CISO、エンジニアリング リーダーシップ	四半期	アラート経路に矛盾がある場合、通知データが不完全になる可能性があります。	OSPO ＋ セキュリティ運用
標準アーティファクトカバレッジ	標準化されたコンプライアンス成果物、通知、または承認された生成パスを使用しているリリースの割合。	法務、エンジニアリング業務	四半期	純粋な自動化指標として扱うのではなく、品質チェックと組み合わせて使用すべきです。	OSPO ＋ リリース エンジニアリング

評価指標	意味	顧客	頻度	注意点	所有者
AIツール来歴情報（来歴評価済み）	組織での使用が承認されたAIコーディングツールのうち、トレーニングデータ、ライセンスへの影響、出力レビュー要件を網羅した出所評価が文書化されているものの割合。付録A.4のAI生成コードポリシー採用指標とは異なり、後者はAIツールが生成するコードを取り巻くポリシー環境を測定するものです。	CTO、法務、CISO	四半期	評価にはレビュー日を明記し、ツールのバージョン変更に応じて再検討する必要があります。評価結果は適用範囲とは別に追跡し、条件付き承認、制限、または却下につながった評価の数を報告することで、適用範囲がガバナンス上の決定を覆い隠さないようにします。	OSPO ＋ 法務および調達

A.4 リスク予測評価指標

表6

リスク予測評価指標

評価指標	意味	顧客	頻度	注意点	所有者
リリース前に特定された高リスク問題	正式な製品リリース前に特定された、ライセンス、出所、ポリシー、またはセキュリティに関連する高リスクの問題の数。	法務、セキュリティ、リスク委員会	四半期	量そのものは、本質的に良いとか悪いとかいうものではなく、その解釈は発見の質や製品構成によって左右されます。	OSPO ＋ セキュリティまたは法務相談担当
後期段階の発見の傾向	正式リリース後、あるいはその他の開発後期段階で初めて発見された問題の傾向。	CTO、COO、リスク リーダーシップ	四半期	後期段階は一貫して定義されなければなりません。	OSPOプログラムリーダー
政策勧告の発行レート	この指標は、OSPOの業務量ではなく、外部の変化に対するOSPOの対応力を測定するものです。 規制、エコシステム、またはガバナンスの状況変化に対応して発行された正式な勧告、ガイダンスノート、または政策説明の数。	法務、セキュリティ、取締役会リスク委員会	四半期または年次	規制や生態系が安定している環境下では、低い税率が適切である可能性がある。規制の大幅な変更（例えば、2027年までのCRA実施期間）や、生態系の大きな混乱が生じている期間に低い割合が続くことは、外部監視が不十分であることを示す警告サインです。この指標は絶対値としてではなく、外部イベントの状況との関連で解釈してください。発行される各勧告には、その発令を促した具体的なトリガーを明記する必要があります。	OSPO責任者

評価指標	意味	顧客	頻度	注意点	所有者
問題検出から決定までの平均時間	問題の特定から次の行動（承認、緩和、置換、エスカレーション、フォーク、貢献、または却下）に関する正式な決定までの経過時間の中央値または平均値。	エンジニアリングリーダーシップ、法務、セキュリティ	月次 または 四半期	複雑な問題には、よりが長い時間を要するのが適切である。個々の数値よりも傾向の方が重要です。	OSPO業務 リーダー
AIが生成したコード ポリシーの採用（エンジニアリング チーム）	AIコーディング ツールの使用および本番コード ベースへの導入前のAI生成コードのレビューに関する、文書化され周知されたポリシーを持つエンジニアリング チームの割合。付録A.3のAIツール承認カバレッジ指標（ツール自体の評価状況を測定するもの）とは異なります。	法務、 CTO、CISO	四半期	ポリシーの存在は必ずしも実施を意味するものではありません。遵守状況を確認するには、最近のAI支援による貢献事例をサンプリングしてレビューする必要があります。この指標を初めて公開する前に、エンジニアリング チームを定義し、合意しておく必要があります。定義は報告期間を通じて安定しているべきです。	OSPO ＋ 法務 ＋ エンジニアリング リーダーシップ

A.5 戦略的影響力評価指標

表7

戦略的影響力のための指標

評価指標	意味	顧客	頻度	注意点	所有者
戦略的な貢献の整合性	製品、プラットフォーム、またはロードマップの優先事項に明確に関連付けられた、外部への資材提供またはエンゲージメント活動の割合。	CTO、製品戦略、CEO	四半期または年次	何が「整合している」とみなされるかを判断するための、簡潔な評価基準が必要です。	OSPO ＋ 製品またはアーキテクチャ リーダーシップ
生態系の表現範囲	組織が正式な代表者を擁し、継続的な関与を行い、または指定スポンサーシップを行っている優先エコシステムの数または割合。	CTO、戦略リーダーシップ	年次	存在感と影響力は同じではありません。その重要性に関する物語と組み合わせましょう。	OSPO責任者 または 標準化リーダー
依存度影響比	組織が以下の条件のうち少なくとも1つを満たす、重要なオープンソースプロジェクトへの貢献度： • 少なくとも1名の従業員がメンテナー、コミッター、またはTSCの役割を担い、過去6か月間に実質的な技術的貢献を行っていること； • 組織が、プロジェクトのガバナンスに直接関連するワーキング グループまたは財団プログラムを後援しており、その関係に責任を負う社内担当者を指名していること； • 組織の技術的貢献が承認され、下流の保守またはセキュリティの負担を測定可能な形で軽減し、その結果を文書化していること（内部文書がまだ確立されていない場合は、メンテナーまたは財団からの第三者による裏付けが必要。これは、実質的な貢献をしているにもかかわらず文書化が不十分な組織を不利にしないためである） 受動的なメンバーシップ、カンファレンスのスポンサーシップ、貢献を伴わない参加は対象外です。	CTO、 戦略、リスク管理	年次	分母（ビジネス上重要なオープンソース プロジェクト）は、指標を初めて公開する前に、アーキテクチャ リーダーシップと定義し、合意しておく必要があります。 この定義は毎年見直されるべきです。	OSPO ＋ アーキテクチャ または エコシステムリーダー

リソース

- Linux Foundation Research and TODO Group. **The 2025 State of OSPOs and Open Source Management**. 2025.
- Linux Foundation Research and TODO Group. **The 2024 State of OSPOs and Open Source Management**. 2024.
- Linux Foundation Research and TODO Group. **The 2023 State of OSPOs and OSS Initiatives.** 2023.
- Hoffmann, M., Nagle, F., and Zhou, Y. **The Value of Open Source Software**. Harvard Business School Working Paper 24-038, January 2024.
- Nagle, F., Powell, K., Zitomer, R., and Wheeler, D. A. **Census III of Free and Open Source Software: Application Libraries**. Linux Foundation, OpenSSF, and Laboratory for Innovation Science at Harvard, December 2024.
- Linux Foundation and TODO Group. **The Lifecycle of an Open Source Program Office: From Inception to Strategic Pivoting**. 2005
- Linux Foundation. **Measuring the Economic Value of Open Source**. 2023.
- Linux Foundation. **The Evolution of the Open Source Program Office (OSPO)**. 2023.
- Linux Foundation Research and OpenSSF. **Addressing Cybersecurity Challenges in Open Source Software**. June 2022.
- Linux Foundation and CNCF. **2024 Cloud Native Security Report**. September 2024.
- GitHub, Linux Foundation, and Harvard Laboratory for Innovation Science. 2024 **Open Source Software Funding Report**. December 2024.
- GitHub. **Octoverse 2024**. November 2024.
- Sonatype. **10th Annual State of the Software Supply Chain Report**. October 2024.
- Synopsys. **2024 Open Source Security and Risk Analysis Report**. February 2024.
- Black Duck Software. **2025 Open Source Security and Risk Analysis Report**. February 2025.
- McKinsey & Company. **Open Source in the Age of AI**. 2024.
- CHAOSS Project. **Community Health Analytics in Open Source Software**.
- CHAOSS Project. **CHAOSS Practitioner Guide: Assessing Viability**.
- Basili, V. R., Caldiera, G., and Rombach, H. D. **The Goal Question Metric Approach. In Encyclopedia of Software Engineering**, John Wiley and Sons, 1994.
- ISO/IEC 5230:2020. Information technology, **OpenChain Specification. International Organization for Standardization**, 2020. (See also the **OpenChain adoption checklist**.)
- European Union. **Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements** (Cyber Resilience Act). Official Journal of the European Union, 20 November 2024. Entered into force 10 December 2024.

フィードバック

入念な校閲を行っても、誤植や不正確な記述が残っている可能性があります。誤りにお気づきの場合、またはフレームワークの修正や改善案をお持ちの場合は、著者まで直接ご連絡ください。

謝辞

著者は、LF ResearchのHilary Carter氏とAnna Hermansen氏、Linux FoundationのOpen Source Project ManagerであるAna Jiménez Santamaría氏、そしてOpen Source Strategy ConsultantのDawn Foster氏による本レポートのレビューと貴重なご意見に感謝いたします。また、OSPO分野の発展における基礎的な活動と継続的なリーダーシップに対し、TODO Groupに敬意を表します。

免責事項

本報告書に表明されている見解は、著者個人のものであり、著者が現在または過去に所属していた組織や雇用主の見解を反映するものではありません。

著者について

Ibrahim Haddad博士は、Head of Infotainment Engineering at Volvo Carsであり、同社の次世代車載インフォテインメント ソフトウェアの開発を統括しています。

Volvo Carsに入社する前は、Linux FoundationでVice President of AI Strategic Programsを務め、LF AI & Dataを率いるとともに、PyTorch FoundationのFounding Executive Directorも兼任していました。LF AI & Dataは、70のプロジェクトにわたる9つの加盟組織から77の加盟組織へと規模を拡大し、開発者や組織がオープンソースAIのコーディング、ガバナンス、規模拡大を行える中立的な組織を構築しました。AIモデルのオープン性に関する標準規格であるモデル オープン性フレームワークを共同開発し、効率的で安全、信頼性が高く倫理的な生成型AIオープンソースイノベーションの民主化、発展、普及を促進するGenerative AI Commonsを立ち上げました。

Samsung Research在籍時には、研究開発担当副社長を務め、Open Source Groupを設立し、100名以上のエンジニアを擁する組織へと成長させた。また、Open Connectivity Foundationの共同設立者であり、Vice Presidentに選出されました。

彼の幅広い経歴は、Ericsson Research、Motorola、Palm、Hewlett-Packard、Linux Foundationに及び、エンジニアリング組織の規模拡大、小規模で専門性の高いチームのリーダーシップ、そして高度にマトリックス化された環境における個人貢献者としての経験を有しています。

彼は、共同開発こそがより速く、より良く、より安価なイノベーションへの道であるという信念に基づき、オープンソース開発を積極的に推進してきました。オープンソース ライセンス コンプライアンスの分野における著名な専門家であり、企業コンプライアンス プログラムの設計、設立、運用において豊富な経験を有しています。また、組織が本格的な外部R&D活動を行う上で必要な構造的基盤として、OSPOを長年にわたり提唱してきました。オープンソース戦略、AIガバナンス、エンジニアリング リーダーシップに関する著書7冊、電子書籍18冊、技術レポート150件以上を執筆する多作な著者でもあります。

Haddad博士はConcordia Universityでコンピュータ サイエンスの博士号を優秀な成績で取得し、学業優秀者としてJ. W. McConnell Memorial Graduate FellowshipとConcordia University 25th Anniversary Fellowshipの両方を授与されました。

LinkedIn: https://www.linkedin.com/in/ibrahimhaddad/
Website: https://ibrahimatlinux.com/

THE LINUX FOUNDATION | Research

2021年に設立されたLinux Foundation Researchは、拡大し続けるオープンソース コラボレーションの規模を探求し、新たな技術動向、ベストプラクティス、そしてオープンソース プロジェクトの世界的な影響に関する洞察を提供しています。プロジェクト データベースとネットワークを活用し、定量的・定性的な手法におけるベスト プラクティスに注力することで、Linux Foundation Researchは世界中の組織にとって有益な、オープンソースに関する知見を得るための頼れるライブラリを構築しています。

x.com/linuxfoundation

facebook.com/TheLinuxFoundation

linkedin.com/company/the-linux-foundation

youtube.com/user/TheLinuxFoundation

github.com/LF-Engineering

本著作を引用する場合は、以下の形式で引用してください：Ibrahim Haddad、「Measuring OSPO Value: A Framework for ROI, Resilience, Risk Foresight, and Strategic Influence」、
序文：Ana Jiménez Santamaría、Linux Foundation、2026年6月。

この日本語文書は、英語版を機械翻訳し、Measuring OSPO Value: A Framework for ROI, Resilience, Risk Foresight, and Strategic Influenceの参考訳として、The Linux Foundation Japanが便宜上提供するものです。
翻訳協力：天満 尚二