

# 第3回ワークショップ用ワークシート

## ワーク

OSPO 担当者として OSS の利用、貢献、公開に関して社内ポリシーに準拠していることをどのようにチェックしますか？

リスククリアランスについて自社のプライオリティを考える要素を聞き取ってみましょう。チェックは誰が（誰と）、いつ（タイミング）、どうやって行うのかも明確にしましょう。

準拠を確認する社内ポリシー	チェック方法			
	誰が（誰と）	いつ（タイミング）	どうやって	備考

## コンプライアンス例

### 法的・技術的なルールとガバナンスを確立する

- ポリシーの策定：OSS の利用、貢献、公開に関する明確な社内ポリシーをどのように策定するか。
- 法務リスク：OSS ライセンス違反や知的財産権侵害のリスクがどの程度あるか。
- 業界規制：貴社の業界に特有のコンプライアンス要件（金融、医療など）があるか。
- セキュリティ要件：サービスや製品のセキュリティレベルがどの程度求められているか。
- IP の重要性：貴社の IP が事業においてどの程度重要か。
- ベンダー依存度：特定のベンダーに過度に依存しているか。
- レガシーシステム：ベンダーサポートが終了する可能性のあるレガシーシステムが存在するか。
- 監査基準：OSS の採用が、規制要件や監査基準にどのように影響するか。監査の可能性や透明性を確保するためにどのようなプロセスを踏むか。
- 監査の頻度と厳格さ：外部監査の頻度や、要求される透明性のレベル。

# OSPO Stage1 Check List

全3回のワークショップを通して、みなさんが実践してきた内容をふりかえりましょう。

<b>オープンソースコンプライアンスプログラムのブランディングを行う</b>	
今の状況	(未着手 / 着手済 / 完成)
自分の認識	

<b>法的リスクやライセンスを管理し、社員がライセンス条項に従って OSS を使用するための手順やドキュメントを作成する</b>	
今の状況	(未着手 / 着手済 / 完成)
自分の認識	

<b>開発者が新しい製品・サービスを開発するにあたり、OSS を利用する際の判断材料となる教育プログラムを作成する</b>	
今の状況	(未着手 / 着手済 / 完成)
自分の認識	

<b>組織全体でのソフトウェア部品表を作成するため、具体的なソフトウェアインベントリプロセスを設定する</b>	
今の状況	(未着手 / 着手済 / 完成)
自分の認識	

<b>組織全体にわたって、OSS の価値・コンプライアンス・教育・SBOM などの必要性を認識する</b>	
今の状況	(未着手 / 着手済 / 完成)
自分の認識	