

あなたの会社の OSS コンプライアンスは大丈夫？

※OSS:「オープンソースソフトウェア」の略

近年、OSS は、家電や通信機器、PC やソフトウェア製品、クラウドサービスなど、様々なところで利用されています。OSS とは、通常、その OSS の開発者¹がライセンス（使用許諾条件）を提示して、インターネットなどで公開しているソフトウェアです。したがって、利用者は、このライセンスに記載された条件を守ったうえで、その OSS を自由に複製したり、改変したり、さらに他者へ配布したりすることができます。ただし、OSS の開発者は一切の責任を負わない条件で公開していますので、OSS を利用する際には、様々なトラブルに対処できるようにしておくことが大切です。

まずは、あなたの会社がビジネスで OSS を利用しているか、そして、きちんと管理できているかを確認してみましょう。

OSS を利用しているか、確認してくださいね。



1. OSS のライセンスを守ろう！

OSS を入手して、自社のビジネスで利用する場合は、その OSS の開発者が定めたライセンスを調査して、その条件を守ることができるかどうかを確認することが大切です。

ライセンスを守って使ってくださいね。



ライセンスは、開発者が自由に決められますので、その内容には様々なものがあります。よくある条件としては、例えば、OSS を誰かに配布する場合は、ライセンスを添付してください、とか、著作権の情報を残しておいてください、といったものがあります。中には、OSS のバイナリを提供する場合、OSS のソースコードも提供してください、とか、OSS と結合したソフトウェアを配布する場合はその全体を OSS にしてください、といった条件のものもあります。

あなたの会社で利用している OSS のライセンスの条件を確認してみましょう。

2. OSS を渡す相手にも情報を提供しよう！

OSS を誰かに渡したら、受け取った人も OSS のライセンスを守る必要があります。また、バグや脆弱性などのトラブルが発生した場合には対処できるようにしておくことも大切です。したがって、OSS を製品に組み込んだり、受託開発したものと一緒にお客様へ提供したりする場合は、そこで利用した OSS の名称やバージョン、ライセンスの情報など、お客様が OSS のライセンスを守り、トラブルに対処するために必要な情報を提供することが大切です。

OSS の情報を提供します。



3. ライセンス違反の影響は大きい！

うちの会社の評判がガタ落ちだあ。



OSS の開発者が提示したライセンスを守らずに、その OSS を製品などに利用した場合、その製品のお客様からライセンス違反を指摘されたり、インターネットに掲載されたりして、会社の信用を損なうことがあります。

また、OSS の開発者から著作権侵害であるとして訴訟を起こされた場合、差止請求や損害賠償請求を求められることもあります。

このような事態を避けるためには、製品などを出荷する前に、その中で OSS を利用していないか、利用している場合は、きちんとライセンスを守り、必要な情報が記載されているか、といったことを確認することが大切です。

¹ 開発者が他者へ著作権を譲渡している場合は、開発者以外の著作権者がライセンスを提示します。

4. バグや脆弱性に対応できるようにしよう！

OSSに限らず、ソフトウェアにはバグや脆弱性が見つかることがあります。これらを放置していると、インターネット経由であなたの会社の秘密情報や個人情報など、大切な情報が盗み出されるおそれがあります。

OSSの開発者は一切の責任を負わない条件でOSSを公開していますので、OSSの利用者は、脆弱性やバグが発生した場合に備えて、これらの情報を収集し、対処できるようにしておくことが大切です。



5. 修正したら OSS の開発者（コミュニティ）へ提供しよう！

バグを修正したので、
もとの OSS 開発者へ
提供します。



OSS のバグや脆弱性、あるいはドキュメントの誤りなどを修正した場合、もとの OSS の開発者へ提供することをお勧めします。同じ OSS を利用する人にも有用ですし、将来、バージョンアップ版を利用するときに、バグや脆弱性が残ったままになっていると、また、同じ修正をしなければなりません。

したがって、修正部分を OSS の開発者へ提供することは、自社の効率化にも役立つのです。

6. OSS の管理体制を確認しよう！

OSS のライセンスを守り、きちんとバグや脆弱性などのトラブルにも対応できるようにするためには、会社の組織として OSS の管理体制を整えておくことが大切です。

あなたの会社では、OSS を管理するための適切な方針があるか、また、その内容に以下が含まれているかをチェックしてみてください。

- (1) 利用する OSS のライセンスを漏れなく調査できていますか？
 - 調査するためのツールを利用することをお勧めします。
- (2) OSS を採用するときに、ライセンスを守れることを確認していますか？
 - ライセンスの内容を理解できないときに、誰に相談できるかも確認してください。
- (3) 開発したソフトウェアや他社から調達した部品に、認識していない OSS が含まれていないかを確認していますか？
 - 調査するためのツールを利用することをお勧めします。
 - 他社から調達する場合、OSS の確認方法を事前に他社と合意しておきましょう。
- (4) 利用した OSS のライセンスを守り、お客様へ情報提供できていることを確認していますか？
 - 確認作業を開発部門以外の第三者でもチェックすると、より確実です。
- (5) どの製品に何の OSS を利用したか、管理できていますか？
 - 会社として一元管理することで、問題発生時の対応が早くなります。
- (6) 利用した OSS に脆弱性やバグが発生した場合、情報を把握できますか？
 - 誰が、どうやって情報を入手するかを確認しておきましょう。
- (7) OSS の開発者（コミュニティ）へ投稿する際の社内ルールがありますか？
 - OSS を修正した場合は、もとの OSS 開発者へ提供することをお勧めします。
- (8) トラブル発生時（ライセンス違反、脆弱性の発生など）の対応方法や相談窓口が明確ですか？
 - 社内外を含め、どこに相談できるかを確認しておきましょう。

これでバッチリ！



これらの OSS の管理体制をドキュメント化して、関係者の間で共通認識しておくことが大切です。

作成元：OpenChain Japan Work Group
<https://openchain-project.github.io/OpenChain-JWG/>