THE LINUX FOUNDATION

Understanding Open Source Technology & US Export Controls

オープンソース技術と米国の輸出規制について

Open development enables global collaboration: a guide for companies using and developing open source technology

オープン開発がグローバル コラボレーションを可能にする：オープンソース技術を使用・開発する企業のためのガイド

A Publication of The Linux Foundation | July 2020

www.linuxfoundation.org

One of the greatest strengths of open source development is how it enables collaboration across boundaries. Open source collaboration occurs transparently, publicly, and across organizational boundaries: individual developers, academics, and employees across the globe can come together and build an open technology that is greater than any of them could individually produce.

オープンソース開発の最大の強みの 1 つは、境界を越えたコラボレーションを可能にする手法にあります。オープンソース コラボレーションは、高度な透明性をもって、公的に、かつ、組織の境界を越えて行われます。世界中の開発者、大学などの研究者、企業従業員が協力するので、彼らのいづれかが単独で成し遂げることのできるものよりも優れたオープン技術を構築できます。

Open source collaboration also occurs across geographic boundaries: people and organizations from a multitude of countries around the world bring their unique perspectives and strengths to build together in the open, and to release the results to all.

オープンソース コラボレーションは、地理的な境界を越えて行われることもあります。世界中のさまざまな国の人々や組織が独自の視点と強みを持ち寄り、公的に共同開発し、その成果をすべての人に公開します。

Because open source development is a global activity, it necessarily involves making available software across national boundaries. Some countries' export control regulations may require taking additional steps to ensure that an open source project is satisfying obligations under local laws. This article briefly describes the Export Administration Regulations of the United States and discusses how they apply to open source communities developing technology in global collaboration. In this article, we will generically refer to "open source" as any technology or software where the source is made publicly available. Open source as a creation model has evolved to cover more than just software technology. Open source now includes a wide range of open technology segments such as hardware designs, microprocessor instruction set architectures, specifications, data models, protocols, standards and any other technology that groups are collaborating to build publicly, in the open.

オープンソース開発はグローバルな活動なので、国境を越えてソフトウェアを利用できるようにする必要があります。一部の国の輸出管理規制では、オープンソース プロジェクトが現地の法律に基づく義務を果たすことを保証するために、追加的な措置を必要とする場合があります。この記事では、米国の Export Administration Regulations（輸出管理規制：EAR）について簡単に説明し、グローバル コラボレーションで技術開発するオープンソース コミュニティに対して、どのように規制が適用されるかについて論じます。この記事は、ソースが公的に入手可能（publicly available）な技術やソフトウェアを総称して「オープンソース」と呼ぶことにします。技術創造モデルとしてのオープンソースは、単なるソフトウェア技術以上のものをカバーするように進化しています。今日、オープンソースには、ハードウェア設計、マイクロプロセッサ命令セット アーキテクチャ、技術仕様、データ モデル、プロトコル、技術標準、その他の技術など、関心を同じくする人々が公的に共同開発する幅広いオープン テクノロジー セグメントが含まれています。

The US Export Administration Regulations

The primary source of United States federal government restrictions on exports are the Export Administration Regulations, or EAR. The EAR is published and updated regularly by the Bureau of Industry and Security (BIS) within the US Department of Commerce.[1] The EAR applies to all items "subject to the EAR," and may control the export, re-export or transfer (in-country) of such items.

Under the EAR, "export" has a broad meaning. Exports can include not only the transfer of a physical product from inside the US to an external location, but also other actions. For example, releasing technology to someone other than a US citizen or lawful permanent resident within the United States is deemed to be an export,[2] as is making available software for electronic transmission that can be received by individuals outside the US.

At first this may seem alarming for open source communities, but the good news is open source technologies that are published and made publicly available to the world are not subject to the EAR. Therefore, open source remains one of the most accessible models for global collaboration.

In the following sections, we will explain why concerns over the United States export control regulations are generally not a problem for the open source model and discuss how the EAR generally does not apply to the export of open source software with a few example situations. We will then address two subject matter areas in certain circumstances: first, open source software that includes encryption functionality; and second, open source software that implements neural network-driven geospatial analysis training functionality. Finally, we will suggest some best practices for open source communities to consider in their projects.

米国輸出管理規制

米国連邦政府による輸出規制の主な拠り所は、EAR (Export Administration Reguraltions) です。EARは、米国商務省の産業安全保障局 (Bureau of Industry and Security: BIS) によって定期的に公開され、更新されています。[1] EARは「EAR対象」と定めたすべての品目に適用され、その品目の輸出、再輸出、または (国内での) 移転を管理します。

EAR においては、「輸出」は広い意味を持ちます。輸出には、米国内から国外への物理的物品の移転だけでなく、その他の活動も含まれることがあります。たとえば、米国市民または合法的な永住者以外の者に米国内で技術を提供することは輸出とみなされ[2]、また、米国外の個人が受信できる電子送信用のソフトウェアを利用可能にすることも同様です。

一見、これはオープンソース コミュニティにとって厄介なことのように見える思えるかもしれませんが、幸いなことに、世界中に公開されて公的に入手可能なオープンソース技術は、EAR の対象になりません。そのため、オープンソースは、グローバル コラボレーションのための最もアクセスしやすいモデルの 1 つとしてその地位を保ち続けています。

以下のセクションでは、米国の輸出管理規制に関する懸念がオープンソース モデルに、通常、問題にならない理由を説明し、さらに、いくつかの状況を例として挙げながら、どのような仕組みによってオープンソース ソフトウェアの輸出に EAR が一般的に適用されないのか論じます。次に、ある特定の状況において規制が適用される 2 つの分野について説明します。1 つ目は、暗号化機能を含むオープンソース ソフトウェアで、もう1つは、ニューラルネットワーク駆動の地理空間分析訓練機能を実装するオープンソース ソフトウェアです。最後に、オープンソース コミュニティがプロジェクトで考慮すべきベストプラクティスをいくつか提案します。

1 Currently available at / こちらを参照：**https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear**

2 See § 730.5(c), currently available at / 「輸出」についてはこちらの§730.5(c)を参照：**https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.730_15&rgn=div8**; see definition of "foreign person" in § 772.1, currently available at / 「外国人」の定義についてはこちらの§772.1を参照：**https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.772_11&rgn=div8**

Applying the EAR to Open Source Software

The EAR defines the scope of certain items, including software and technology, that may be subject to export restrictions. The EAR provides for Export Control Classification Numbers, or "ECCNs," for different classifications of items, including software and technology. Some items are subject to the EAR, meaning that they are inside the EAR's scope and may only be exported if: the EAR permits the export without a license, a license exception applies, or a license to export is obtained.

This is where open source technologies are advantageous because the EAR explicitly exempts most software and technology made available as open source. Some items are specifically not "subject to" the EAR at all, meaning that they are *"outside the regulatory jurisdiction of the EAR and are not affected by these regulations."*[3] Specifically, the EAR states in § 734.3(b)[4], *"The following are not subject to the EAR:"* and then lists, *"Information and 'software' that: (i) Are published, as described in § 734.7".* The reference to § 734.7 is important as this section states materials that are "published" are not subject to the EAR. Specifically, the EAR § 734.7 states[5],

> *... unclassified "technology" or "software" is "published," and is thus not "technology" or "software" subject to the EAR, when it has been made available to the public without restrictions upon its further dissemination...*

Open source software from the Linux Foundation and project communities we work with is "published" as described in EAR § 734.7.

オープンソース ソフトウェアへの EAR の適用

EAR は、ソフトウェアや技術など、輸出規制の対象となる特定の品目の範囲を定義しています。EAR では、ソフトウェアや技術など、さまざまな分類の品目に対応する輸出規制分類番号（Export Control Classification Number: ECCN）を提供しています。ある品目が EAR の対象であるということは、「当該品目が EAR の規制範囲内にあり、「EAR が輸出許可なしの輸出を認める場合」、「許可例外が適用される場合」、または、「輸出許可が取得された場合」においてのみ輸出できるということを意味します。

オープンソース技術が有利なのはここです。というのは、EAR は、オープンソースとして公的に入手可能なほとんどのソフトウェアと技術を明示的に免除しているからです。一部の品目は、はっきりと EAR の「対象」ではないとされており、それは、「EAR の規制管轄権の外にあり、これらの規制の影響を受けない」ということを意味しています。[3] 具体的には、EAR は、§ 734.3(b)[4] で「次のものは EAR の対象ではない」とし、その後に「(i) § 734.7 に記載した状態にて公開されている情報および『ソフトウェア』」を列挙しています。§ 734.7 への言及は重要です。なぜなら、このセクションは、「公開」された物件（情報、ソフトウェアなど）は EAR の対象ではないと述べているからです。EAR § 734.7 [5] は、はっきりと次のように述べています。

> ... それの普及時に、制約なく公的に入手可能となる場合、機密扱いでない「技術」または「ソフトウェア」は「公開」されているものとし、したがって EAR の対象となる「技術」または「ソフトウェア」とはならない ...

Linux Foundation や私たちが協力しているプロジェクト コミュニティのオープンソース ソフトウェアは、EAR § 734.7 に記述されているように「公開」されています。

3 See § 734.2(a)(1), currently available at /「EAR対象」については、§734.2(a)(1)を参照：**https://www.ecfr.gov/cgi-bin/text-idx?node=pt15.2.734&rgn=div5#se15.2.734_12**

4 See § 734.3(b), currently available at /「EAR対象外」については、§734.3(b)を参照：**https://www.ecfr.gov/cgi-bin/text-idx?node=pt15.2.734&rgn=div5#se15.2.734_13**

5 See § 734.7, currently available at /「公開」については、§734.7を参照：**https://www.ecfr.gov/cgi-bin/text-idx?node=pt15.2.734&rgn=div5#se15.2.734_17**

The following typical scenarios (but not an exhaustive list) are not subject to the EAR because “open source” is “published”:

- Open source software that is published publicly is not subject to the EAR
- Open source specifications that are published publicly are not subject to the EAR
- Open source files that describe the designs for hardware that are published publicly are not subject to the EAR
- Open source software binaries that are published publicly are not subject to the EAR

The key word is the word “published.” For the purposes of the EAR, if the open source technology is publicly available without restrictions upon its further dissemination, then it is “published” and therefore “not subject to” the EAR. It would be a major shift in existing policy for the EAR to be changed to make “published” software and technology subject to EAR restrictions, and we are not aware of any current discussion for such a change.

The US position that publicly available software or technology is not subject to export control is also not specific to the US regulations, but also includes the European Union.

Additionally, activities that do not relate to software, technology or other items within the EAR’s scope are not subject to the EAR. Non-technical collaboration falls into this category: meetings about business matters, event planning, marketing, and similar activities are not subject to the EAR, because they are outside its scope.

To meet the requirement of “published” under the EAR, open source communities may need to take one additional step if the project includes encryption technology.

以下の典型的なシナリオ（網羅したものではない）では「オープンソース」が「公開」されているため、EAR の対象ではありません。

- 公開されているオープンソース ソフトウェアは EAR の対象ではない
- 公開されているオープンソース仕様は EAR の対象ではない
- 公開されているハードウェア設計を記述したオープンソース ファイルは、EAR の対象ではない
- 公開されているオープンソース ソフトウェアのバイナリは EAR の対象ではない

キーワードは、「公開（published）」です。EAR の主旨として、オープンソース技術が、その普及時に、制約なく公的に入手可能（publicly available without restrictions）になるのであれば、それは「公開」されたものとみなされ、したがって EAR の「対象」ではありません。「公開」されたソフトウェアおよび技術を EAR 規制の対象とするように変更することは、既存のポリシーの大きな変更であり、いまのところそのような変更のための議論の徴候は見られません。

公的に入手可能なソフトウェアや技術が輸出規制の対象ではないという米国の立場は、米国の規制に特有のものではなく、同様の立場の国・地域として欧州連合も含まれます。

さらに、EAR の規制範囲内のソフトウェア、技術、その他の品目に関連しない活動は、EAR の対象にはなりません。非技術的なコラボレーションはこのカテゴリーに分類されます。ビジネスに関連した事柄、イベント計画、マーケティング、および類似の活動に関するミーティングは、EAR の規制範囲外であるため、EAR の対象にはなりません。

プロジェクトに暗号化技術が含まれている場合、EAR の「公開」という要件を満たすために、オープンソース コミュニティはもう 1 つのステップを踏む必要があるかもしれません。

Encryption

One primary EAR subject area of focus for software developers is encryption. The EAR regulates exports of certain encryption software and technology. The definition of "encryption software" is very broad and can include software that merely activates or enables encryption features in another software or hardware product.[6] For software implementations of standard encryption functionality, including encryption hardware when represented in software design files, the most common ECCN classification is 5D002. If encryption software is "subject to" the EAR, then in order to export it anywhere except to Canada, one would need to first confirm that an exception applies, or request and obtain a license from BIS to permit the export.

However, before considering whether an exception or export license is necessary, the first question should be: is the encryption software "subject to" the EAR at all?

Encryption source code classified under ECCN 5D002 is not subject to the EAR if both (1) it is "publicly available," and (2) an email notification has been sent for it to the addresses listed in that section.[7]

For the first part of the test, the meaning of "publicly available" refers to the EAR's definition of "published," which includes public dissemination by posting on the Internet on sites available to the public.[8] Given this, the first part of the test should be met for all fully-public open source software projects: if the project's source code is openly available on the Internet, then it should be considered "publicly available."

§734.7

暗号化

ソフトウェア開発者にとって、注意すべき EAR 規制対象の主なテーマの 1 つは暗号化です。EAR は、一定の暗号化ソフトウェアや技術の輸出を規制しています。「暗号化ソフトウェア」の定義は非常に広く、別のソフトウェア製品やハードウェア製品の暗号化機能を起動または有効にするだけのソフトウェアを含めることもあります。[6] 標準的な暗号化機能のソフトウェア実装に対する最も一般的な ECCN 分類は 5D002 です。なお、このソフトウェア実装には、ソフトウェア設計ファイルで表現されている暗号化ハードウェアも含まれます。暗号化ソフトウェアが EAR の「対象」である場合、カナダ以外のどこかにそれを輸出するためには、許可例外が適用されることを確認するか、あるいは、BIS に輸出許可を申請して取得する必要があります。

しかし、許可例外または輸出許可が必要かどうかを検討する前に行うべき最初の質問は次のとおりです。
暗号化ソフトウェアはそもそも EAR の「対象」なのか？

ECCN 5D002 に分類された暗号ソースコードは、(1) それが「公的に入手可能」であり、かつ (2) そのセクションに記載されたアドレス宛てに E メール通知が送信されている場合、EAR の対象ではありません。[7]

上記の条件の最初の部分では、「公的に入手可能」の意味は、EAR の「公開」の定義を参照しており、これには、不特定多数が利用可能なインターネット サイト上に掲載することによる公衆への普及を含みます。[8] このため、条件の最初の部分は、完全に公開されたすべてのオープンソース ソフトウェア プロジェクトで満たされるはずです。つまり、プロジェクトのソースコードがインターネット上で公開されている場合、そのソースコードは「公的に入手可能」と見なされるでしょう。

6 See §772.1, currently available at /「暗号化ソフトウェア」の定義は、§772.1（用語定義）を参照：
https://www.ecfr.gov/cgi-bin/text-idx?node=pt15.2.772&rgn=div5

7 See §742.15(b), currently available at /公的に入手可能な暗号化ソースコード」については、§742.15(b)を参照：
https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.742_115&rgn=div8

8 See §734.7, currently available at /「公開」については、§734.7を参照：
https://www.ecfr.gov/cgi-bin/retrieveECFR?n=pt15.2.734&r=PART&ty=HTML#se15.2.734_17
§734.3(b)(3), currently available at /「EAR対象外」については、§734.3(b)(3)を参照：**https://www.ecfr.gov/cgi-bin/retrieveECFR?n=pt15.2.734&r=PART&ty=HTML#se15.2.734_13**

For the second part of the test, it is additionally necessary to send an email to two specified addresses, one at BIS and the other at the US National Security Agency (NSA). The email should include the URL of the publicly-available code (or a copy of the code itself). An updated notification should be sent later if the previously-provided URL or copy has changed.[9]

Finally, after the two-part test is satisfied, then its corresponding object code counterpart is also not subject to the EAR.[10]

At The Linux Foundation, the source code for all of our projects, including encryption software, is publicly available, and we have provided email notices as described above. We also make copies of these email notices publicly available for viewing on the LF's website.[11] As a result, the Linux Foundation's project source code and corresponding object code are not subject to EAR encryption restrictions.

Please keep in mind that this applies only to the open source project itself. Downstream redistributors of modified project code, or products derived from it, where the source code is not publicly available would still need to evaluate their own compliance with the EAR (just as with any other software that they export).

2つ目の条件として、指定された2つのアドレス（1つはBIS、もう1つは米国国家安全保障局（NSA））にEメールを送信する必要があります。Eメールには、公的に入手可能なコードのURL（またはコード自体のコピー）を含める必要があります。以前に提示したURLまたはコピーが変更された場合は、更新通知を後で送信すべきです。[9]

最後に、上記の2つの条件が満たされると、対応するオブジェクトコードもEARの対象になりません。[10]

The Linux Foundationでは、暗号化ソフトウェアを含むすべてのプロジェクトのソースコードが公的に入手可能となっており、上記のEメール通知も行っています。また、これらのEメール通知のコピーをThe Linux FoundationのWebサイトで閲覧できるようにしています。[11] そのため、The Linux Foundationのプロジェクトのソースコードとそれに対応するオブジェクト コードは、EAR暗号化の制約を受けません。

これは元のオープンソース プロジェクトにのみ適用されることに注意してください。改変されたプロジェクト コードのダウンストリーム再配布、あるいは、それから派生した製品は、ソースコードが公的に入手可能になっていないと、（輸出する他のソフトウェアと同様に）EARに関するそれぞれの企業のコンプライアンス手順に照らす必要があります。

9 See § 742.15(b), currently available at /「公的に入手可能な暗号化ソースコード」については、§742.15(b)を参照：
https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.742_115&rgn=div8

10 See / 以下のサイトを参照：**https://www.bis.doc.gov/index.php/policy-guidance/encryption/223-new-encryption**

11 See / The Linux Foundationが掲載した送信メールを参照：
https://www.linuxfoundation.org/export/

Neural network-driven geospatial analysis training

On January 6, 2020, BIS announced a new EAR rule that immediately went into effect. This rule established EAR controls over a specific kind of geospatial imagery software that is specially designed for training a Deep Convolutional Neural Network[12] to automate the analysis of geospatial imagery and point clouds. The rule clarifies that a "point cloud" refers to a collection of data points defined by a given coordinate system, also known as a digital surface model.[13] Although the rule went into effect immediately upon publication, it remains subject to comment and may continue to develop or change. In any case, if it is publicly available software (e.g. open source software) then it still would not be subject to the EAR, as described above.

Some public portrayals of the new rule may have implied that it imposed broad prohibitions on geospatial imagery software, or even on artificial intelligence / machine learning software as a whole. That is not the case.

The scope of the rule actually appears to be quite narrowly tailored. It applies only to that which specifically includes all of the aspects described above. Furthermore, in order to be subject to the new EAR rule, the software must also include all of the following functionality:

1. Provides a graphical user interface that enables the user to identify objects (e.g., vehicles, houses, etc.) from within geospatial imagery and point clouds in order to extract positive and negative samples of an object of interest;

ニューラル ネットワーク駆動の地理空間分析訓練機能

2020 年 1 月 6 日、BIS は新たな EAR 規則を発表し、直ちに施行されました。この規則は、深層畳み込みニューラル ネットワーク（Deep Convolutional Neural Network）[12] の訓練（train）用に特別に設計され、地理空間画像と点群の解析の自動化を行う特定の種類の地理空間画像ソフトウェアに対する EAR のコントロールを確立するものです。この規則で「点群」とは、デジタル サーフェス モデルとも呼ばれ [13]、特定の座標系によって定義されたデータ点の集合を指します。この規則は公表と同時に施行されましたが、引き続きコメント受けつけの対象となっており（訳注：コメント締め切りは 2020 年 3 月 6 日）、今後、さらに発展したり、変更される可能性があります。いずれにしても、それが公的に入手可能なソフトウェア (例えば、オープンソース ソフトウェア) であれば、上述のように EAR の対象にはなりません。

この新しい規則に対する一般的な見方の中には、地理空間画像ソフトウェアに対して、あるいは、人工知能 / 機械学習ソフトウェア全体に対してさえも、広範な禁止を課したものとみなしているものもあるかもしれません。しかし、そうではありません。

この規則の適用範囲は、実際にはかなり狭く作られているように見えます。本規則は、上述の諸側面のすべてを具体的に含むものにのみ適用されます。さらに、新しい EAR 規則の対象となるには、ソフトウェアに次のすべての機能が含まれている必要があります。

1. 対象物の正例および負例を抽出するために地理空間画像および点群内からオブジェクト (車両、家屋など) を識別するグラフィカル ユーザー インターフェイスを提供する。

12 Although "Deep Convolutional Neural Network" is not defined in the regulation, for background information see, e.g., / 発表文書に「深層畳み込みニューラル ネットワーク」の定義はないが、背景情報については、以下のいずれかのサイトを参照：
https://en.wikipedia.org/wiki/Convolutional_neural_network ;
https://pathmind.com/wiki/convolutional-network

13 See 85 FR 459, currently available at / 発表された米国政府官報「85FR459」については、以下のサイトを参照：
https://www.federalregister.gov/d/2019-27649/p-12

2. Reduces pixel variation by performing scale, color, and rotational normalization on the positive samples;

3. Trains a Deep Convolutional Neural Network to detect the object of interest from the positive and negative samples; and

4. Identifies objects in geospatial imagery using the trained Deep Convolutional Neural Network by matching the rotational pattern from the positive samples with the rotational pattern of objects in the geospatial imagery.

If software does not include every one of the aspects and functionality listed above, then it appears that it would not be subject to the new restrictions in their current form. The list of requirements reads very closely to what you might expect a commercial solution provider to deliver as a solution, not as an open source project. In particular the requirement for training would require not only a software project but a training dataset of positive and negative samples that would likely only apply to a specific implementation of the neural network.

There may be some publicly available, open source projects today that implement this functionality. However, even if a new project were to be created today, as long as it is run as a publicly available open source project then it would not be subject to the EAR.

2. 正例に対して、スケール、カラー、および回転の正規化を実行することで、画素のばらつきを減らす。

3. 正例および負例から対象物を検出するように、深層畳み込みニューラル ネットワークを訓練する。

4. 正例の回転パターンを地理空間画像内の対象物の回転パターンとマッチングすることにより、訓練された深層畳み込みニューラル ネットワークを使用して地理空間画像内の対象物を識別する。

ソフトウェアに上記のすべての諸側面と機能が含まれていない場合、現在の形では新しい制限の対象にならないようです。この要件リストは、商用ソリューション プロバイダーがオープンソース プロジェクトとしてではなく、ソリューションとして提供を期待する内容と非常によく似ています。特に、訓練のための要件は、ソフトウェア プロジェクトだけでなく、ニューラル ネットワークの特定の実装にのみ適用される可能性が高い正例および負例の訓練データセットを必要としています。

今日では、この機能を実装した、公的に入手可能なオープンソース プロジェクトがいくつかあるかもしれません。しかし、新しいプロジェクトが今日開設されることになったとしても、それが公的に入手可能なオープンソース プロジェクトとして進められる限り、EAR の対象にはなりません。

Best Practices for Open Source Software Communities

There are a few practices we have learned or developed that may be helpful for all open source communities.

Be Open and Be Public

We often use the word “open” to mean many things: an open source license, open and transparent discussions, open community, openly available source code on a public repository. “Open” may seem an obvious practice for open source communities, but there are some recommendations for communities.

First, communities should strive to keep their technical conversations open and public. If private conversations happen within communities, that’s normal, it is recommended to make the community decisions and outcomes publicly available. It is important for our projects to make information available transparently and publicly as the private exchange of technology or technical information may not meet the “publicly available” standard according to the EAR.

One question that has come up has to do with exchanges of information related to security issues under a security disclosure process. As a best practice, projects may want to consider making exchanges like this public upon availability of fixes, and not limit this information to only the confidential disclosure list.

Exchanging technical ideas and knowledge, and having a technical debate are hallmarks of open source communities where the best technical solutions should rise to the forefront. These exchanges may be uncomfortable to have in public at times, but our communities who strictly

オープンソース ソフトウェア コミュニティのベストプラクティス

私たちが学んだ、あるいは開発した多くの手法は、すべてのオープンソース コミュニティに役立つ可能性があります。

オープンでパブリックに

「オープン」という言葉は、オープンソース ライセンス、オープンで透明性のある議論、オープンなコミュニティ、公開リポジトリ上でオープンに入手可能なソースコード、などいろいろな意味で使われています。「オープン」はオープンソース コミュニティにとっては当たり前のように思えるかもしれませんが、コミュニティに対してはいくつかの推奨事項があります。

第一に、コミュニティは技術的な会話をオープンに公開するよう努力すべきです。 常にあり得ることですが、コミュニティ内でプライベートな会話が行われたとしても、コミュニティの意思決定と結果を公的に入手可能にすることが推奨されます。プロジェクト内における技術や技術情報の私的な交換は、EAR の「公的に入手可能」の基準を満たしていない可能性があるため、オープンソース プロジェクトでは、そのような情報を透明かつ公的に入手可能にすることが重要です。

疑念の 1 つは、セキュリティ問題の発生時、セキュリティ情報開示プロセスの下で行われる情報の交換に関するものです。ベストプラクティスとして、プロジェクトでは、修正プログラムが利用可能になった時点でこのような情報交換を公開することを検討し、この情報を機密情報開示リストだけに限定しないようにするのがよいでしょう。

技術的なアイデアや知識を交換し、技術的な議論を行うことは、オープンソース コミュニティの優れた特徴であり、そこから最良の技術的ソリューションが前面に押し出されます。 こうした交流は、時には公の場で行うのが難しいこともありますが、この原則を厳格に守るコミュニティは、透明で信頼できるコミュニティの

hold to this principle are often the most successful at building transparent and trusting communities. There may be disagreements, but everyone knows the discussion is happening in public and transparently - there are many positive benefits to public, open collaboration beyond just meeting requirements in the EAR.

Deliver encryption notifications

If your open source software project implements or uses encryption functionality classified under ECCN 5D002, you will likely want to deliver a notification of encryption to the BIS and the NSA according to the EAR requirements. EAR § 742.15(b)(2)[14] describes these requirements:

- Send an email to **crypt@bis.doc.gov** and **enc@nsa.gov**.
- The email should contain either the URL of the publicly available encryption source code, or a copy of the source code itself. Typically we would expect that open source projects would select the first option.
- If you provided a URL to a site where you posted the source code on the Internet, you must notify by email again each time the Internet location is changed, but you are not required to notify them of updates or modifications made to the encryption source code at the previously notified location.
- If you provided a copy of the source code, and you update or modify the source code, you must also provide additional copies to each of them each time the cryptographic functionality of the source code is updated or modified.

As you will see in the Linux Foundation's notices,[15] we suggest a few additional details as best practices:

構築に最も成功しています。「意見の相違はあるかもしれないが、議論が公の場で透明に行われていることを誰もが知っている」このようなコミュニティにおいて、公的に行われるオープン コラボレーションには、単に ERA の要件を満たすだけはない大きなメリットがあります。

暗号化に関する通知

オープンソース プロジェクトにおいて、ECCN 5D002 に分類される暗号化機能を実装または使用している場合は、EAR の要件に従って、BIS と NSA に暗号化機能に関する通知を送信する必要があります。EAR § 742.15(b)(2)[14] は、これらの要件を次のように記述しています。

- **crypt@bis.doc.gov** と **enc@nsa.gov** に E メールを送信する。
- E メールには、公的に入手可能な暗号化ソースコードの URL、またはソースコード自体のコピーを含める必要がある。オープンソース プロジェクトは、通常、最初のオプションを選択することが予想される。
- ソースコードを掲載したインターネット サイトの URL を提示した場合、インターネット上の場所が変更されるたびに再度 E メールで通知する必要があるが、以前に提示した場所で暗号化ソースコードが更新または変更されたことを通知する必要はない。
- ソースコードのコピーを提供してあり、そのソースコードを更新または変更する場合、ソースコードの暗号化機能が更新または変更されるたびに、それぞれの送信先にそのコピーを提供する必要がある。

The Linux Foundation の通知でも見ることができますが [15]、以下にベストプラクティスの詳細をいくつか提案します。

14 See §742.15(b), currently available at / 以下のサイトの§742.15(b)を参照：
https://www.ecfr.gov/cgi-bin/text-idx?node=se15.2.742_115

15 **https://www.linuxfoundation.org/export/**

- Make publicly available copies of the notices that were delivered to BIS and NSA, in order to increase transparency and visibility of compliance. This also helps with your community of downstream users who may wonder “do they send notices?” You can prevent concerns by making the notices themselves public.

- Include contact information and, where applicable, the name of the particular legal entity that is responsible for the project.

- Establish a system to ensure that you maintain evidence, for a medium- to long-term period of time, that the notification emails to BIS and NSA were in fact delivered. Relying solely on an individual’s “Sent” mailbox records may not be preferable if a question arises in the future, or if that individual loses access to that Sent mailbox.

If you are unsure whether your open source software project uses encryption functionality, or whether it might in the future, you might also consider delivering a notice out of an abundance of caution.

Ensure corresponding encryption source code is publicly available

If you are distributing publicly available encryption software in object code form, then you will also want to ensure that it is publicly available in source code form as well.

Maintainers of the project, who are most familiar with the project’s code, should review to see if there are instances where encryption functionality is distributed in binary or object code form. Where it is, consider first if that is necessary. Distributing in source code form may be a preferred approach—not only for export compliance

- コンプライアンスの透明性と可視性を高めるために、BIS と NSA に送信した通知のコピーを公開する。 これは、「彼らは通知を送信しているだろうか ?」と疑問に思うダウンストリーム ユーザーのコミュニティにも役立ち、通知自体を公開することで、懸念を回避できる。

- 連絡先情報、さらに、プロジェクトを担当する特定の法務法人があればその名前を含める。

- BIS および NSA への通知メールが実際に送信されたことを示す証拠を中長期的に確実に保持するシステムを確立する。個人の「送信済み」メールボックスの記録のみに依存することは、後で疑義が発生したり、その個人が送信済みメールボックスにアクセスできなくなったりするので、あまり好ましくない。

オープンソース ソフトウェア プロジェクトで暗号化機能が使用されているのか、あるいは、将来使用される可能性があるのかわからない場合は、十分な注意（次項を参照）を払ったうえで、自ら通知を行うことを検討することもできます。

対応する暗号化ソースコードが公的に入手可能なことを確認する

公的に入手可能な暗号化ソフトウェアをオブジェクトコード形式で配布する場合は、ソースコード形式でも公開する必要があります。

プロジェクトのコードに最も精通しているプロジェクトのメンテナーは、暗号化機能がバイナリまたはオブジェクトコード形式で配布されている事例があるかどうかを確認する必要があります。そのような事例がある場合は、まずはそれが必要なのかどうかを検討します。ソースコード形式で配布することは、輸出規制に準拠するためだけでなく、ダウンストリーム ユーザーが「ブラックボックス」バイナリを信頼することに依存せず、ソースコードから自分で簡単にビルドできるようにするためにも、望ましいアプローチです。

purposes, but also so that downstream users are not dependent on trusting a “black box” binary, and can easily build it themselves from source code.

If it is necessary to distribute encryption software in binary or object code form, then ensure that the corresponding source code is publicly available.[16] The easiest way to do this is to make available the source code for that version of the encryption software yourself, as part of the project’s own code. (In fact, depending on the applicable open source license, this may be necessary or at least useful in complying with that open source license as well!)

In addition to manual review, there are[17] some scanning tools with varying degrees of ability to scan source code and detect usage of encryption functionality. No automated scanning tool is likely to be a perfect detector of all applicable uses, but these may be helpful in identifying copies of encryption software in a large codebase.

暗号化ソフトウェアをバイナリまたはオブジェクトコード形式で配布する必要がある場合は、対応するソースコードが公的に入手可能であることを確認します。[16] これを行う最も簡単な方法は、そのバージョンの暗号化ソフトウェアのソースコードをプロジェクトのコードの一部として利用できるようにすることです。（実際、該当するオープンソース ライセンスによっては、そのライセンスに準拠するためにこれが必要になったり、役立ったりします。）

人手によるレビューのほか、ソースコードをスキャンして暗号化機能の使用状況を検出するさまざまなレベルのスキャン ツールもあります。[17] 自動スキャン ツールは、可能なすべての用途に対応する完璧な検出器にはなりませんが、大規模なコードベースで暗号化ソフトウェアのコピーを見つけるのに役立つかもしれません。

16 See / 以下を参照： **https://www.bis.doc.gov/index.php/policy-guidance/encryption/223-new-encryption**

17 See, e.g., Fossology, see under “Export Control Codes” / たとえば以下の Fossology の “Export Control Codes” の項を参照：
https://www.fossology.org/features/ ；
exportctrl from the Software Freedom Law Center / あるいは Software Freedom Law Center の exportctrl “Export-control scanning tools”を参照：
http://code.softwarefreedom.org/cgit/exportctrl/

The Linux Foundation promotes, protects and standardizes Linux by providing unified resources and services needed for open source to successfully compete with closed platforms.

To learn more about The Linux Foundation or our other initiatives please visit us at **www.linuxfoundation.org**