Keylimeを使用したSLE Microのセキュリティ保護

概要

Keylimeは、TPMベースのリモートブートの検証とランタイムの整合性の測定です。

目的

この記事では、SLE MicroでKeylimeを設定および実行する方法について説明します。

所要時間

この記事の理解には25分ほどを要します。

目標

Keylimeの仕組み、設定方法、および実行方法について詳しく理解します。

要件

- SLE Microの実行中のインスタンス。

発行日: 11/12/2025

目次

1 Keylimeを使用したリモート検証

不正な変更からデバイスを保護する機能の要望が強くなるに伴い、セキュリティメカニズムとして「リモート検証(RA)」が広く使用されるようになっています。RAを使用すると、ホスト(クライアント)は、ブートチェーンのステータスと実行中のソフトウェアをリモートホスト(ベリファイア)で認証できます。RAは、公開鍵暗号化(TPM2を使用)と組み合わされることが多いため、送信された情報を読み込めるのは検証を要求したサービスだけであり、データの有効性を検証できます。

SLE Microのリモート検証は、**Keylime**で実装されます。

1.1 用語集

リモート検証テクノロジでは次の用語を使用します。

検証キー(AK)
: データが本物のTPMからのもので、改ざんされていないことを証明するデータ署名キー。

Core Root of Trust for Measurement
: 自身のハッシュと、ブートプロセスの次のステップのハッシュを計算し、測定のチェーンを開始します。

エンドースメントキー(EK)
: TPMの製造時にそれに永続的に埋め込まれる暗号化キー。TPMに保存されているキーの公開部分と証明書を使用して、本物のTPMを認識します。

Integrity Management Architecture (IMA)
: ファイルに対する悪意のある変更を検出する手段を提供するカーネル整合性サブシステム。

メジャーブート
: ブートシーケンスの各コンポーネントで、次のコンポーネントのハッシュを計算したうえで実行をそのコンポーネントに委任する手法。このハッシュは、TPMの1つまたは複数のPCRを拡張した値です。測定が行われた場所と測定内容に関する情報を含むイベントが作成されます。このようなイベントは拡張されたPCR値とともにイベントログに収集され、正常なシステムであることを示す期待値と比較できます。

Platform Configuration Register (PCR)

TPMの内部メモリの中で、ブートレイヤのハッシュなどを保存する場所。PCRは非可逆的操作(`extend`)のみを使用して更新できます。現在のPCR値の署名済みリストは、TPMの`quote`コマンドで取得することができ、このQuoteをサードパーティが検証プロセス中に検証できます。

セキュアブート

ブートプロセスの各ステップでは、次のステップにある実行可能ファイルの暗号署名が確認されます。その確認を経たうえでその実行可能ファイルが実行されます。

Trusted Platform Module (TPM)

自己完結型のセキュリティ暗号プロセッサ。ハードウェアでシステムに搭載されているか、信頼の基点(Root of Trust)として機能するファームウェアに実装されています。TPMは、ブートレイヤのハッシュを保存したPCRを提供します。一般的なTPMは、乱数ジェネレータ、カウンタ、ローカルクロックなどの機能を提供します。また、サポート対象の暗号ハッシュ関数(SHA1、SHA256、SHA384、SHA512)ごとにバンク別にグループ化した24個のPCRを保存します。

注記

デフォルトでは、TPMの使用は無効になっています。したがって、メジャーブートは実行されません。リモート検証を有効にするには、EFI/BIOSメニューでTPMを有効にします。

セキュアペイロード

暗号化したデータを正常なエージェントに配信するメカニズム。ペイロードを使用して、エージェントで使用するキー、パスワード、証明書、設定、スクリプトを提供します。

1.2 Keylimeとは

Keylimeはリモート検証ソリューションであり、TPMを測定の信頼の基点として使用し、リモートノードの状態を監視できます。Keylimeを使用すると、次のようなタスクを実行できます。

- メジャーブート中に、拡張されたPCRを検証する。
- イベントログの分析を作成し、アサーションを設定する。

- リモートシステムで任意のPCR値のアサーションを設定する。
- 開いているファイルまたは実行されたファイルの有効性を監視する。
- 「セキュアペイロード」を使用して、検証済みノードに暗号化データを配信する。
- コンピュータが検証済みの測定に失敗した場合にトリガするカスタムスクリプトを実行する。

1.3 アーキテクチャ

Keylimeは、エージェント、ベリファイア、レジストラ、コマンドラインツール(テナント)で構成されます。エージェントは検証が必要なシステム上に置かれます。ベリファイアとレジストラは、エージェントの登録と検証を実行するリモートシステム上に置かれます。SLE Microではエージェント役割のみがあります。各コンポーネントの詳細については以下の該当するセクションを参照してください。

1.3.1 Keylimeのエージェント

エージェントは、検証を受ける必要があるシステム上で実行されるサービスです。エージェントは、イベントログ、IMAハッシュ、および測定されたブートに関する情報をベリファイアに送信します。その際に、ローカルTPMをデータの有効性の証明者として使用します。

新しいエージェントが開始したときは、まず、そのエージェント自体をレジストラに登録する必要があります。その登録には、接続を確立するためのTLS証明書がエージェントに必要です。TLS証明書はレジストラで生成されますが、手動でエージェントにインストールする必要があります。登録後、エージェントはその検証キーとエンドースメントキーの公開部分をレジストラに送信します。レジストラは、資格情報のアクティベーションプロセスでエージェントにチャレンジで応答します。このプロセスは、エージェントのTPMの検証を目的としています。エージェントが登録されると、それを検証で使用できるようになります。

1.3.2 Keylimeのレジストラ

レジストラを使用して、検証を受ける必要があるエージェントを登録します。レジストラは、エージェントの検証キー、エンドースメントキーの公開部分、およびエンドースメントキー証明書を収集し、エージェントの検証キーがエンドースメントキーに属することを検証します。

1.3.3 Keylimeのベリファイア

ベリファイアはエージェントの実際の検証を行い、必要な検証データをエージェントから継続的に取得します(特に、PCR値、IMAログ、およびUEFIイベントログ)。

2 Podmanを使用したKeylimeワークロードの実行

Keylimeは、リモートノードのヘルスを監視できるリモート検証ソリューションです。「ベリファイア」と「レジストラ」は、リモートシステム上のKeylimeの重要なコンポーネントであり、Keylimeエージェントの登録と検証を実行します。

注記

この記事で説明するコンテナは、Keylimeプロジェクトの一部であるコントロールプレーンサービスの「ベリファイア」と「レジストラ」、および「テナント」コマンドラインツール(CLI)を提供します。

エージェントのインストールと登録を開始する前に、次の手順で説明するように、リモートホスト上でベリファイアとレジストラを準備します。

1. Keylimeワークロードのイメージを特定します。

```
# podman search keylime
[...]
registry.opensuse.org/devel/microos/containers/containerfile/opensuse/keylime-
control-plane
```

2. そのイメージをレジストリから取得します。

```
# podman pull\
  registry.opensuse.org/devel/microos/containers/containerfile/opensuse/keylime-
control-plane:latest
```

3. `keylime-control-plane`ボリュームを作成して、検証プロセス中に必要なデータベースと証明書を永続化します。

```
# podman container runlabel install \
  registry.opensuse.org/devel/microos/containers/containerfile/opensuse/keylime-
control-plane:latest
```

4. コンテナと関連するサービスを開始します。

```
# podman container runlabel run \
  registry.opensuse.org/devel/microos/containers/containerfile/opensuse/keylime-
control-plane:latest
```

keylime-control-planeコンテナが作成されます。ここには、設定されて実行中のレジストラサービスとベリファイアサービスが含まれます。内部では、コンテナは、デフォルト値を使用してポート8881、8890、および8891をホストに公開します。ファイアウォール設定を検証し、これらのポートへのアクセスを許可します。また、テナントCLIで必要になるため、コンテナ間の通信も許可します。

ヒント

Keylimeサービスを停止する場合は次のコマンドを実行します。

```
# podman kill keylime-control-plane-container
```

2.1 Keylimeサービスの監視

ホスト上で実行しているコンテナのステータスを取得するには次のコマンドを実行します。

```
# podman ps
```

Keylimeサービスのログを表示するには次のコマンドを実行します。

```
# podman logs keylime-control-plane-container
```

2.2 テナントCLIの実行

テナントCLIツールはコンテナに含まれており、ホストのファイアウォールがKeylimeサービスによって公開されるポートに干渉しなければ、同じイメージを使用して実行できます。次に例を示します。

```
# podman run --rm \
-v keylime-control-plane-volume:/var/lib/keylime/ \
keylime-control-plane:latest \
keylime_tenant -v 10.88.0.1 -r 10.88.0.1 --cert default -c reglist
```

2.3 Keylime証明書の抽出

Keylimeコンテナを初めて実行したときに、いくつかのエージェントが必要とする証明書がそのコンテナのサービスによって作成されます。コンテナから証明書を抽出して、エージェントの`/var/lib/keylime/cv_ca/`ディレクトリにコピーする必要があります。

```
# podman cp \
keylime-control-plane-container:/var/lib/keylime/cv_ca/cacert.crt
.# scp cacert.crt
AGENT_HOST:/var/lib/keylime/cv_ca/
```

ヒント

エージェントのインストールの詳細については3項 「Keylimeエージェントのインストール」を参照してください。

3 Keylimeエージェントのインストール

Keylimeは、リモートノードのヘルスを監視できるリモート検証ソリューションです。Keylimeエージェントは、検証が必要なシステム上で実行され、イベントログ、IMAハッシュ、および測定されたブートに関する情報をベリファイアに送信するサービスです。

Keylimeエージェントは、デフォルトではSLE Microに存在しないため、手動でインストールする必要があります。このエージェントをインストールするには次の手順に従います。

1. 次のように`rust-keylime`のパッケージをインストールします。

   ```
   # transactional-update pkg in rust-keylime
   ```

   続いてシステムを再起動します。

2. エージェントのデフォルトの設定を調整します。

   a. 指定した変更を収めた新しい設定ファイルを保存するディレクトリを`/etc/keylime/agent.conf.d/`に作成します。デフォルトの設定は`/usr/etc/keylime/agent.conf`に保存されていますが、このファイルは今後のシステム更新で上書きされることがあるので、このデフォルトのディレクトリへの保存はお勧めできません。

   ```
   # mkdir -p /etc/keylime/agent.conf.d
   ```

b. 新しいファイル/etc/keylime/agent.conf.d/agent.confを作成します。

```
# cat << EOF > /etc/keylime/agent.conf.d/agent.conf
 [agent]

 uuid = "d111ec46-34d8-41af-ad56-d560bc97b2e8"❶ registrar_ip =
 "<REMOTE_IP>"❷
 revocation_notification_ip = "<REMOTE_IP>"❸
 EOF
```

❶ エージェントを実行するたびに固有の識別子が生成されます。このオプションでは、その識別子に特定の値を定義できます。

❷ レジストラのIPアドレス。

❸ ベリファイアのIPアドレス。

c. /etc/keylime/ディレクトリの所有者をkeylime:tssに変更します。

```
# chown -R keylime:tss /etc/keylime
```

d. /etc/keylime/ディレクトリに対する許可を次のように変更します。

```
# chmod -R 600 /etc/keylime
```

3. CAで生成された証明書をエージェントノードにコピーします。エージェントノードで次の手順を実行します。

a. 証明書のディレクトリを用意します。

```
# mkdir -p /var/lib/keylime/cv_ca
```

b. エージェントに証明書をコピーします。

```
# scpCERT_SERVER_ADDRESS:/var/lib/keylime/cv_ca/cacert.crt /var/lib/keylime/
cv_ca
```

c. 証明書の所有者をkeylime:tssに変更します。

```
# chown -R keylime:tss /var/lib/keylime/cv_ca
```

4. keylime_agent.serviceを開始して有効にします。

```
# systemctl enable --now keylime_agent.service
```

4 Keylimeエージェントの登録

Keylimeは、リモートノードのヘルスを監視できるリモート検証ソリューションです。Keylimeエージェントは、検証が必要なシステム上で実行され、イベントログ、IMAハッシュ、および測定されたブートに関する情報をベリファイアに送信するサービスです。

新しいエージェントを登録するには、テナントCLIを使用するか、ベリファイアの設定を編集します。ベリファイアのホスト上でテナントを使用して、次のコマンドを実行します。

```
# keylime_tenant -v 127.0.0.1 \
  -tAGENT \❶
  -u UUID \❷
  --cert default \
  -c add
  [--include PATH_TO_ZIP_FILE]❸
```

❶ `AGENT`は、登録するエージェントのIPアドレスです。

❷ `UUID`は、エージェント固有の識別子です。

❸ `include`オプションで渡したファイルを使用してエージェントにシークレットペイロードのデータが配信されます。詳細については、5項 「Keylimeセキュアペイロード」を参照してください。

登録済みエージェントを列挙するには、ベリファイアのホスト上で次のように**`reglist`**コマンドを使用します。

```
# keylime_tenant -v 127.0.0.1 \
  --cert default \
  -c reglist
```

登録済みエージェントを削除するには、次のように、`-t`オプションと`-u`オプション、および`-c delete`コマンドを使用してエージェントを指定します。

```
# keylime_tenant -v 127.0.0.1 \
  -tAGENT \
 -u UUID \
  -c delete
```

5 Keylimeセキュアペイロード

Keylimeは、リモートノードのヘルスを監視できるリモート検証ソリューションです。

5.1 セキュアペイロードとは

Keylimeのセキュアペイロードを使用すると、正常なエージェントに暗号化データを配信できます。ペイロードを使用して、後工程でKeylimeエージェントが使用するキー、パスワード、証明書、設定、スクリプトを提供します。

5.2 セキュアペイロードの動作

セキュアペイロードは、`zip`ファイルに収めてエージェントに配信されます。このファイルには、シェルスクリプト`autorun.sh`を収めておく必要があります。このスクリプトは、エージェントが適切に登録および検証されている場合にのみ実行されます。`zip`ファイルを配信するには、**`keylime_tenant`**コマンドで`--include`オプションを指定します。

たとえば、次の`autorun.sh`スクリプトは、ディレクトリ構造を作成して、そこにSSHキーをコピーします。関連する`zip`アーカイブには、これらのSSHキーが記述されている必要があります。

```
> cat autorun.sh
#!/bin/bash

 mkdir -p /root/.ssh/
 cp id_rsa* /root/.ssh/
 chmod 600 /root/.ssh/id_rsa*
 cp /root/.ssh/id_rsa.pub /root/.ssh/authorized_keys
```

6 KeylimeのIMA追跡の有効化

Keylimeは、リモートノードのヘルスを監視できるリモート検証ソリューションです。**Integrity management architecture** (IMA)は、ファイルに対する悪意のある変更を検出する手段を提供するカーネル整合性サブシステムです。

IMAを使用すると、アクセス先ファイルのハッシュがカーネルによって計算されます。その後、このハッシュを使用して、TPMのPCR 10を拡張し、さらにアクセスされたファイルのリストも記録します。ベリファイアは、PCR 10の署名付き予測をエージェントに要求して、すべてのアクセス先ファイルのログ記録をファイルハッシュ付きで取得できます。続いて、ベリファイアは、承認済みファイルのローカル許可リストとアクセス先ファイルを比較します。いずれかのハッシュが認識されない場合、システムは安全ではないと見なされ、取り消しイベントがトリガされます。

Keylimeで情報を収集できるようになるまで、IMA/EVMを有効にしておく必要があります。このプロセスを有効にするには、エージェントのカーネルを、`ima_appraise=log`パラメータと`ima_policy=tcb`パラメータを指定してブートします。

1. `/etc/default/grub`にあるパラメータで`GRUB_CMDLINE_LINUX_DEFAULT`オプションを更新します。

```
GRUB_CMDLINE_LINUX_DEFAULT="ima_appraise=log ima_policy=tcb"
```

2. 次のコマンドを実行して`grub.cfg`を再生成します。

```
# transactional-update grub.cfg
```

3. システムを再起動します。

上記の手順では、カーネルでデフォルトのIMAポリシーを使用しています。監視するファイルが多すぎるために長大なログが作成されるのを回避するには、新しいカスタムポリシーを作成します。詳細については、Keylime documentation (https://keylime-docs.readthedocs.io/en/latest/user_guide/runtime_ima.html)を参照してください。

想定されるハッシュが示されるようにするには、エージェントを登録するときに**`keylime_tenant`**コマンドで`--allowlist`オプションを指定します。除外されたファイルまたは無視されたファイルを確認するには、**`keylime_tenant`**コマンドで`--exclude`オプションを指定します。

```
# keylime_tenant --allowlist
    -v 127.0.0.1 \
    -uUUID
```

7 詳細情報

- Keylimeのホームページはhttps://keylime.devです。
- Keylimeの最新ドキュメントはhttps://keylime.readthedocs.io/en/latest/にあります。
- IMA/EVMの概要についてはhttps://en.opensuse.org/SDB:Ima_evm#Introductionを参照してください。
- 新しいカーネルIMAポリシーを作成する方法についてはhttps://keylime-docs.readthedocs.io/en/latest/user_guide/runtime_ima.htmlを参照してください。

8 法的事項

A GNUフリー文書利用許諾契約書(GFDL)

0. 序文

この利用許諾契約書の目的は、マニュアル、テキストブック、またはその他の機能的で有用な文書を、自由という意味で「フリー」にすることです。つまり、そのような文書を、変更の有無や商用非商用に関わらず、コピーまたは再配布する実効的な自由をすべての人々に保証することです。第二に、本利用許諾契約書は、作者または発行者が他者によって行われた変更について責任を負わないとともに、その著作物の功績が確保されるように意図されています。

本利用許諾契約書は、「コピーレフト」(著作物を自由に複製および改変できるようにすること)の一種であり、文書の派生著作物は、それ自体が同じ意味においてフリーでなければなりません。フリーソフトウェア向けに考慮されたコピーレフト利用許諾であるGNU一般公衆利用許諾契約書(GPL)を補足するものです。

弊社は、この利用許諾契約書をフリーソフトウェアのマニュアルに使用するために設計しました。それは、フリーソフトウェアにはフリーマニュアルが必要であるためです。つまり、フリープログラムには、そのソフトウェアと同じ自由を提供するマニュアルが付属しなければなりません。ただし、本利用許諾契約書は、ソフトウェアマニュアルに制限されるものでは

ありません。主題であるか否か、または印刷された本として発行されるか否かに関わらず、任意のテキスト著作物に使用することができます。本利用許諾契約書は、その目的が指示または参照に置かれている著作物に主に使用することを推奨します。

1. 適用範囲と定義

本利用許諾契約書は、この利用許諾の条項に従って頒布できることを定めた著作権者の通告が記載されている任意のメディアにおけるマニュアルまたは他の著作物に適用されます。そのような通告は、その著作物をここに記載されている条件に従って使用するための世界的な無償の利用許諾を無期限で付与します。次に示す「文書」は、そのような任意のマニュアルまたは著作物を指します。その公衆ユーザはいずれも被許諾者であり、「利用者」と呼ばれます。利用者は、著作権法に従った許可が必要になるような方法で著作物を複製、変更または頒布する場合に、利用許諾を受け入れます。

文書の「変更された版」とは、そのまま複製されるか、変更または別の言語に翻訳された(またはその両方)文書あるいはその一部を含んだ著作物のことです。

「二次セクション」は、文書の発行者または作者と文書の全体的な主題(または関連事項)との関係のみを示す文書の名前付き付録または前付け部分です。総体的な主題に直接関わる内容は含まれていません。(したがって、文書が部分的に数学のテキストブックになっている場合、二次セクションでは数学について説明されない場合があります)。関係には、主題または関連事項との歴史的なつながり、あるいはそれらに関する法的、商的、哲学的、倫理的、政治的位置付けが含まれる場合があります。

「不変セクション」は、文書が本利用許諾契約書の条件の下でリリースされる旨を述べている通告において、そのタイトルが不変セクションのものとして指定されている、ある特定の二次セクションです。セクションが、すでに説明した二次セクションの定義に一致しない場合は、不変として指定することはできません。文書には、不変セクションが含まれない場合があります。文書で不変セクションを特定しない場合、不変セクションは含まれません。

「カバーテキスト」とは、文書が本利用許諾契約書の条件の下でリリースされる旨を述べている通告において、表カバーテキストまたは裏カバーテキストとして列挙されている、ある一定の短い文章のことです。表カバーテキストは、最大で5語、裏カバーテキストは、最大で25語によって構成できます。

文書の「透過的な複製」とは、その仕様が一般の利用者にとって入手可能で、一般的なテキストエディタまたは一般的な描画プログラム(画素で構成される画像用)、あるいは広く使用されている図面エディタ(図面用)で文書を直接改訂するのに適した形式で表される機械可読の複製のことです。テキストフォーマッタへの入力またはテキストフォーマッタへの入力に適したさまざまな形式への変換に適していることも前提になります。読者による以後の変更を阻止または妨げるようにマークアップまたはマークアップのない状態が調整されている、他の点では

透過的なファイル形式で行われた複製は、透過的な複製ではありません。イメージ形式は、相当量のテキストに使用されている場合、透過的ではありません。「透過的」ではない複製は、「不透明」と呼ばれます。

透過的な複製に適した形式として、マークアップのないプレーンなASCII、Texinfo入力形式、LaTeX入力形式、一般に取得可能なDTDを使用するSGMLまたはXML、標準に準拠したHTML、人為的変更用のPostScriptまたはPDFがあります。透過的なイメージ形式には、PNG、XCF、JPGが含まれます。不透明な形式には、独自のワードプロセッサのみで読み取りおよび編集を行える独自の形式、DTDまたは処理(またはその両方)ツールを一般に取得できないSGMLまたはXML、機械生成HTML、出力のみを目的として一部のワードプロセッサによって作成されるPostScriptまたはPDFが含まれます。

「タイトルページ」とは、印刷された本の場合、タイトルページ自体、および本利用許諾契約書でタイトルページに表示することが要求されるマテリアルを読みやすいように保持するために必要な以降のページのことを指します。そのようなタイトルページがない形式の著作物の場合、「タイトルページ」は、本文の開始部分に先行する、著作物のタイトルを最も顕著に表している部分の近くにあるテキストのことを指します。

「XYZという表題の付いた」セクションとは、そのタイトルが正確にXYZになっているか、またはXYZを別の言語に翻訳しているテキストに続いてカッコ付きのXYZが含まれている文書の名前付きサブユニットのことです。(ここで、XYZは、次に示すように、「謝辞」、「献辞」、「推薦」、「履歴」などの特定のセクション名を表します)。文書を変更するときに、そのようなセクションの「タイトルを保存する」とは、この定義に従って「XYZという表題の付いた」セクションが残されることを表します。

文書では、本利用許諾契約書が文書に適用される旨を述べている通告の付近に保証の放棄を含めることができます。保証の放棄条項は、本利用許諾契約書内の参照によって、保証の放棄に関してのみ組み込まれると見なされます。つまり、これらの保証の放棄条項がもつ可能性のある他のいかなる含意も無効であり、本利用許諾契約書の意味にまったく影響を与えません。

2. そのままの複製

利用者は、商用か否かを問わず、任意のメディアにおいて文書を複製または頒布することができます。その際に、本利用許諾契約書、著作権表示、および本利用許諾契約書が文書に適用される旨を述べる利用許諾通告をすべての複製で再生し、本利用許諾契約書の条件に他のいかなる条件も追加しないことが前提条件になります。利用者は、技術的手段によって、作成または頒布する複製の読み込みまたはさらなる複製を妨げたり、制御したりすることはできません。ただし、複製と引き換えに対価を受け取ることができます。十分に大量の複製を頒布する場合は、セクション3の条件に従う必要もあります。

すでに述べた同じ条件に従って複製を貸与したり、複製を公開したりすることもできます。

3. 大量の複製

発行する文書の印刷した複製(または、通常、印刷したカバーをもつメディアに含まれた複製)が 100部を超え、文書の利用許諾通告でカバーテキストを必要とする場合は、すべてのカバーテキスト(表カバーの表カバーテキスト、裏カバーの裏カバーテキスト)を明瞭かつ読みやすく記載したカバーに文書の複製を同封する必要があります。また、両方のカバーでは、これらの複製の発行者として、利用者を読みやすい状態で明確に識別しなければなりません。表カバーには、フルタイトルを記述し、タイトルのすべての語が同等に目立つようにする必要があります。カバーには他のマテリアルを追加することもできます。カバーに限って変更を行った場合の複製は、文書のタイトルが保持されていて、これらの条件を満たしている限り、他の点に関してそのままの複製と見なすことができます。

いずれかのカバーで、必要なテキストが多すぎて、読みやすい状態に収まらない場合は、列挙されている最初の部分(問題なく収まる分)を実際のカバーに記載し、残りの部分を隣接ページに入れます。

文書の不透明な複製を100部以上公開または頒布する場合は、それぞれの不透明な複製とともに機械可読の透過的な複製を含めるか、それぞれの不透明な複製内あるいはその複製とともに、ネットワークの一般利用者が標準的な一般ネットワークプロトコルを使用して、追加マテリアルのない文書の完全な透過的複製をダウンロードするときにアクセスできるコンピュータネットワークの場所を明記する必要があります。後者のオプションを使用する場合は、不透明な複製の大量頒布を開始するときに十分慎重な手順を取り、この透過的な複製が、その版の不透明な複製を最後に一般頒布した後(直接またはエージェントや小売業者を通じて)少なくとも1年間、指定した場所で継続的にアクセス可能となるように配慮する必要があります。

大量の複製を再頒布する時点よりもかなり前に、文書の作者に連絡して、文書の更新版を提供する機会を与えることが要求されますが、必須ではありません。

4. 変更

文書の変更された版を、すでに述べた第2項および第3項の条件に従って複製および頒布することができます。その際は、本利用許諾契約書に確実に従って、変更された版をリリースし、変更された版が文書の役割を担うようにして、その複製を所要する任意の利用者に変更された版の頒布および変更の利用許諾を与えることが前提になります。また、変更された版で次のことを行う必要があります。

A. タイトルページ(カバーがある場合はカバー上も含める)で、文書、および以前の版の文書(以前の版がある場合は、その旨、文書の履歴セクションに列挙する)と識別されるタイトルを使用します。前の版と同じタイトルは、その版の元の発行者が許可を与えた場合に、使用することができます。

B. タイトルページ上に、この要件から解放されない限り、変更された版において変更の著者としての責任を担う1人以上の人またはエンティティとともに、文書の筆頭著者を少なくとも5人、作者として列挙します(5人に満たない場合は、その筆頭著者のすべて)。

C. タイトルページ上に、変更された版の発行者の名前を、発行者として記載します。

D. 文書のすべての著作権表示を保持します。

E. 変更に関する適切な著作権表示を、他の著作権表示の隣に追加します。

F. 著作権表示の直後に、本利用許諾契約書の条項に従って変更された版を利用するための許可を一般利用者に与える利用許諾通告を、次の補遺に示す形式で含めます。

G. その利用許諾通告に、不変セクションの全リスト、および文書の利用許諾通告で指定されている必須カバーテキストを保持します。

H. 本利用許諾契約書の変更されていない複製を含めます。

I. 「履歴」という表題のセクションを保持して、そのタイトルを保持し、タイトルページに記載されているとおりに、変更された版のタイトル、年度、新しい作者、発行者を少なくとも示す項目を追加します。文書に履歴というセクションがない場合は、そのタイトルページに記載されているとおりに文書のタイトル、年度、作者、発行者を示すセクションを作成し、前の文章に記載されているとおりに変更された版を示す項目を追加します。

J. 文書の透過的な複製に一般利用者がアクセスできるように文書で指定されている場合は、そのネットワークの場所、およびその文書の基盤となった前の版に対応して文書で指定されているネットワークの場所を保持します。これらは、「履歴」セクションに配置することができます。文書自体よりも4年以上前に発行された著作物の場合、または参照されているその版の元の発行者が許可を与えている場合は、そのネットワークの場所を省略することができます。

K. 「謝辞」または「献辞」という表題のセクションの場合は、そのセクションのタイトルを保持し、セクション内に、それぞれの貢献者謝辞またはその中の献辞(またはその両方)のすべての内容と意味合いを保持します。

L. 文書のすべての不変セクションを保持し、そのテキストおよびタイトルを未変更のままにします。セクション番号またはそれと同等の要素は、セクションタイトルの一部と見なされません。

M. 「推薦」という表題の任意のセクションを削除します。そのようなセクションは、変更された版に含めることはできません。

N. 既存のセクションのタイトルを変更して、「推薦」という表題にしたり、タイトルが不変セクションと矛盾したりしないようにします。

O. 保証の放棄を保持します。

変更された版に、二次セクションと見なされ、文書から複製されたマテリアルを含まない新しい前付けセクションまたは付録が含まれる場合は、これらの一部またはすべてを任意に「不変」として指定することができます。これを行うには、変更された版の利用許諾表示内で列挙されている不変セクションにそのタイトルを追加します。これらのタイトルは、他のすべてのセクションタイトルと異なっている必要があります。

「推薦」という表題のセクションを追加することができますが、その際は、変更された版のさまざまな当事者による推薦以外の要素が含まれていないことが前提になります。たとえば、校正者によるコメント、または文が標準的な信頼できる定義として組織によって承認されていることを示すという宣言文などが相当します。

表カバーテキストとしての最大5語の短い文、および裏カバーテキストとしての最大25語の短い文を、変更された版のカバーテキストのリストの終わりに追加できます。表カバーテキストの短い1文および裏カバーテキストの短い1文のみを、1つのエンティティが追加できます(またはエンティティによって行われた調整を通じて)。文書に、利用者または利用者が関わる同じエンティティによって行われた調整を通じて前に追加された同じカバーのカバーテキストがすでに含まれている場合は、別のものを追加することはできませんが、古いものを置き換えることができます。ただし、その古いものを追加した前の発行者から明示的な許可を得る必要があります。

文書の作者および発行者は、本利用許諾契約書により、その名前を得るために使用したり、変更された版の推薦を主張または暗示したりする許可を与えるものではありません。

5. 文書の結合

文書は、すでに述べた変更された版に関するセクション4の条件に従って、本利用許諾契約書の下でリリースされた他の文書と結合することができます。その際は、その組み合わせの中に、元の全文書のすべての不変セクションを未変更のまま含めて、そのすべてを結合された著作物の不変セクションとしてその利用許諾表示に列挙し、そのすべての保証の放棄を保持することが前提となります。

結合された著作物には、本利用許諾契約書の複製を1つのみ含める必要があります。複数の同一の不変セクションは、単一の複製で置き換えることができます。同じ名前だが内容の異なる複数の不変セクションがある場合は、そのような各セクションのタイトルを固有なものにし

ます。その際は、その終わりに、カッコ付きで、そのセクションの元の作者または発行者の名前(既知の場合)、あるいは固有の番号を追加します。不変セクションのリスト内のセクションタイトルには、結合された著作物の利用許諾表示の場合と同じ調整を加えます。

組み合わせでは、さまざまな元の文書の「履歴」という表題のセクションを結合して、1つの「履歴」というセクションを構築する必要があります。同じように、「謝辞」という表題のセクション、および「献辞」という表題のセクションも結合します。「推薦」という表題のすべてのセクションを削除する必要があります。

6. 文書のコレクション

文書および本利用許諾契約書の下でリリースされた他の文書から成るコレクションを作成して、さまざまな文書に含まれる本利用許諾契約書の個々の複製を、コレクションに含まれる単一の複製で置き換えることができますが、他のすべての点での各文書のそのままの複製に関する本利用許諾契約書の規則に従うことが前提になります。

そのようなコレクションから単一の文書を抽出して、その文書を本利用許諾契約書に従って個々に頒布することができますが、その際は、本利用許諾契約書の複製を抽出した文書に挿入して、その文書のそのままの複製に関するその他のすべての点で、本利用許諾契約書に従う必要があります。

7. 独立した著作物の集積

文書またはその派生物を他の個別および独立した文書または著作物とともに、ストレージまたは頒布メディア内またはそのボリューム上に蓄積することを「集積」と呼びます。その場合は、個々の著作物の許可を超えてその蓄積の利用者の法的権限を制限することに、蓄積による著作権を使用しないことが前提になります。文書が集積に含まれる場合、本利用許諾契約書は、それ自体が文書の派生著作物ではない集積内の他の著作物に適用されません。

セクション3のカバーテキスト要件が文書のこれらの複製に適用可能であり、文書が集積全体の半分に満たない場合は、文書のカバーテキストを、集積内の文書のカバー、または文書が電子形式の場合は、電子的な同等のカバーに配置することができます。それ以外の場合は、集積全体の印刷されたカバー上に表示する必要があります。

8. 翻訳

翻訳は一種の変更と見なされるため、セクション4の条件に従って文書の翻訳を配布することができます。不変セクションを翻訳で置き換えるには、著作権者からの特別な許可が必要ですが、これらの不変セクションの元のバージョンのほかに、一部またはすべての不変セクションの翻訳を含めることができます。本利用許諾契約書、文書内のすべての利用許諾表示、お

よび保証の放棄の翻訳を含めることができますが、その際は、本利用許諾契約書の元の英語版、およびそれらの利用許諾表示と保証の放棄の元の版も含めることが前提になります。本利用許諾契約書、利用許諾表示、または保証の放棄の翻訳と元の版との間に不一致がある場合は、元の版が優先されます。

文書内のセクションに、「謝辞」、「献辞」、または「履歴」という表題が付いている場合は、そのタイトルを保持する(セクション1)ための要件(セクション4)により、通常は実際のタイトルを変更する必要があります。

9. 終了

利用者は、本利用許諾契約書に明示的に記載されている形態を除き、文書を複製、改変、二次利用許諾、および頒布してはなりません。別の方法で文書を複製、改変、二次利用許諾、または頒布しようとするのは無効であり、本利用許諾契約書の下で利用者の権利は自動的に消滅します。ただし、本使用許諾の下で利用者から複製物または権利を受領した関係者は、条項を遵守している限り、権利が消滅することはありません。

10. 本利用許諾契約書の将来の改訂

フリーソフトウェア財団は、GNUフリー文書利用許諾契約書(GFDL)の新版または改訂版を随時公表することがあります。そのような新版は、性格的には現行版と似たものになりますが、新たな問題や懸案事項に対応するために細部が異なる可能性があります。https://www.gnu.org/copyleft/を参照してください。

本利用許諾契約書の各版には、区別するための版番号が設定されます。文書に、それに適用される本利用許諾契約書の特定の版番号と「後継版」が指定されている場合、利用者は、選択によって、その指定された版の条項またはフリーソフトウェア財団から公開される後継版の条項(ドラフトではない)に従うことになります。文書に、本利用許諾契約書の版番号が指定されていない場合、利用者は、フリーソフトウェア財団からこれまでに公開された任意の版(ドラフトではない)を選択することができます。

補遺: 本利用許諾書をご使用の文書に使用する方法

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

不変セクション、表カバーテキスト、および裏カバーテキストがある場合は、
「with...Texts」の行を次のように置き換えます。

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

カバーテキストのない不変セクションが含まれている場合、またはこの3つの他の組み合わせの場合は、その2つの代替要素をマージして状況に合わせます。

文書にプログラムコードの重要な例が含まれている場合は、GNU一般公衆利用許諾契約書(GPL)などの選択したフリーソフトウェアの利用許諾に従って、これらの例を平行してリリースし、フリーソフトウェアでのその利用を許可することを推奨します。