

SELinuxのトラブルシューティング

概要

SELinuxが`enforcing`モードになっているシステムでアクセス拒否が発生し、アプリケーションを正しく実行できない場合があります。 `audit2allow`または`setroubleshoot`を使用して、使いやすい方法で拒否メッセージを分析できます。

目的

この記事では、SELinuxが原因で発生するアクセス拒否を、システムのセキュリティを低下させることなく解決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30分ほどを要します。

目標

詳しく説明されているツールの1つを使用してSELinuxの拒否をデバッグできるようになります。

要件

- SELinuxが有効になっている実行中のシステム。

発行日: 11/12/2025

目次

- 1 /var/log/audit/audit.logファイル 3
- 2 **audit2allow**を使用した/var/log/audit/audit.logの分析 5
- 3 **setroubleshoot**を使用したAVCメッセージの分析 7
- 4 法的事項 12
- A GNUフリー文書利用許諾契約書(GFDL) 13

1 /var/log/audit/audit.logファイル

デフォルトでは、SELinuxが原因で何かが動作していない場合、この旨を示すログメッセージが/var/log/audit/audit.logファイルに送信されます。



注記: 空の/var/log/audit/audit.log

空の/var/log/audit/audit.logが表示される場合、通常はauditdサービスが実行されていないことを意味します。この場合は、次の手順を実行します。

1. auditdサービスを開始します。

```
> sudo systemctl start auditd
```

2. 次のコマンドを使用して、システムのターゲットでサービスを有効にします。

```
> sudo systemctl enable auditd
```

/var/log/audit/audit.logファイルには、アクセス拒否、サービスイベントなどのメッセージが保存されます。

例 1: 「/etc/audit/audit.logの行の例」で、/var/log/audit/audit.logの内容の部分的な例を確認できます。

例 1: /etc/audit/audit.logの行の例

```
type=DAEMON_START msg=audit(1348173810.874:6248): auditd start, ver=1.7.7 format=raw
kernel=3.0.13-0.27-default audit=0 pid=4235 subj=system_u:system_r:auditd_t res=success
type=AVC msg=audit(1348173901.081:292): avc: denied { write } for
pid=3426 comm="smartd" name="smartmontools" dev=sda6 ino=581743
scontext=system_u:system_r:fsdaemon_t tcontext=system_u:object_r:var_lib_t tclass=dir
type=AVC msg=audit(1348173901.081:293): avc: denied { remove_name } for pid=3426
comm="smartd" name="smartd.WDC_WD2500BEKT_75PVMT0-WD_WXC1A21E0454.ata.state~" dev=sda6
ino=582390 sccontext=system_u:system_r:fsdaemon_t tcontext=system_u:object_r:var_lib_t
tclass=dir
type=AVC msg=audit(1348173901.081:294): avc: denied { unlink } for pid=3426
comm="smartd" name="smartd.WDC_WD2500BEKT_75PVMT0-WD_WXC1A21E0454.ata.state~" dev=sda6
ino=582390 sccontext=system_u:system_r:fsdaemon_t tcontext=system_u:object_r:var_lib_t
tclass=file
type=AVC msg=audit(1348173901.081:295): avc: denied { rename } for pid=3426
comm="smartd" name="smartd.WDC_WD2500BEKT_75PVMT0-WD_WXC1A21E0454.ata.state" dev=sda6
ino=582373 sccontext=system_u:system_r:fsdaemon_t tcontext=system_u:object_r:var_lib_t
tclass=file
```

```
type=AVC msg=audit(1348173901.081:296): avc: denied { add_name } for pid=3426
comm="smartd" name="smartd.WDC_WD2500BEKT_75PVMTO-WD_WXC1A21E0454.ata.state~"
scontext=system_u:system_r:fsdaemon_t tcontext=system_u:object_r:var_lib_t tclass=dir
type=AVC msg=audit(1348173901.081:297): avc: denied { create } for pid=3426
comm="smartd" name="smartd.WDC_WD2500BEKT_75PVMTO-WD_WXC1A21E0454.ata.state"
scontext=system_u:system_r:fsdaemon_t tcontext=system_u:object_r:var_lib_t tclass=file
type=AVC msg=audit(1348173901.081:298): avc: denied { write open } for pid=3426
comm="smartd" name="smartd.WDC_WD2500BEKT_75PVMTO-WD_WXC1A21E0454.ata.state" dev=sda6
ino=582390 scontext=system_u:system_r:fsdaemon_t tcontext=system_u:object_r:var_lib_t
tclass=file
type=AVC msg=audit(1348173901.081:299): avc: denied { getattr } for pid=3426
comm="smartd" path="/var/lib/smartmontools/smartd.WDC_WD2500BEKT_75PVMTO-
WD_WXC1A21E0454.ata.state" dev=sda6 ino=582390 scontext=system_u:system_r:fsdaemon_t
tcontext=system_u:object_r:var_lib_t tclass=file
type=AVC msg=audit(1348173901.309:300): avc: denied { append } for pid=1316
```

単一のメッセージは次のようになります。

```
type=AVC msg=audit(1348173901.081:299): avc: denied { getattr } for pid=3426
comm="smartd" path="/var/lib/smartmontools/smartd.WDC_WD2500BEKT_75PVMTO-
WD_WXC1A21E0454.ata.state" dev=sda6 ino=582390 scontext=system_u:system_r:fsdaemon_t
tcontext=system_u:object_r:var_lib_t tclass=file
```

メッセージのすべての行をセクションに分割できます。たとえば、最終行のセクションは次のようになります。

type=AVC:

SELinuxに関連する監査ログのすべての行は、type=AVCのような、タイプの識別情報で始まります。type=SYSCALLのメッセージが別のタイプのメッセージの後に続いていて、msgの値が同じである場合、メッセージでイベントに関する詳細情報が提供されている場合があることに注意してください。

msg=audit(1348173901.309:300):

タイムスタンプです。エポック時間(1970年1月1日からの経過秒数)で記述されています。エポック時間表記のドットまでの部分に対して`date -d`を使用すると、そのイベントの発生日時を確認できます。

```
> date -d @1348173901
Thu Sep 20 16:45:01 EDT 2012
```

avc: denied { append }:

拒否された具体的なアクション。この場合、ファイルへのデータの追加がシステムによって拒否されました。監査ログファイルを参照中に、システムの他のアクション(write open、getattrなど)を確認できます。

`for pid=1316:`

アクションを開始したコマンドまたはプロセスのプロセスID。

`comm="rsyslogd":`

PIDに関連付けられていた特定のコマンド。

`name="smartmontools":`

アクションの対象の名前。

`dev=sda6 ino=582296:`

関係のあるファイルのブロックデバイスとiノード番号。

`scontext=system_u:system_r:syslogd_t:`

ソースコンテキスト。これはアクションの開始者のコンテキストです。

`tclass=file:`

対象のクラスの識別情報。

2 `audit2allow`を使用した`/var/log/audit/audit.log`の分析

`/var/log/audit/audit.log`内のイベントを自身で解釈する代わりに、`audit2allow`コマンドを使用できます。

このコマンドは、`/var/log/audit/audit.log`のわかりにくいログメッセージを分析するのに役立ちます。`audit2allow`のトラブルシューティングセッションは、常に3つの異なるコマンドで構成されます。まず、`audit2allow -w -a`を使用して、監査情報をより読みやすい方法で表示します。デフォルトでは、`audit2allow -w -a`は`audit.log`ファイルを処理します。`audit.log`ファイル内の特定のメッセージを分析する場合は、そのファイルを一時ファイルにコピーして次のコマンドで分析します。

```
> sudo audit2allow -w -i FILENAME
```

例 2: 監査メッセージの分析

```
> sudo audit2allow -w -i testfile
type=AVC msg=audit(1348173901.309:300): avc: denied { append } for pid=1316
comm="rsyslogd" name="acpid" dev=sda6 ino=582296
scontext=system_u:system_r:syslogd_t tcontext=system_u:object_r:apmd_log_t tclass=file
```

原因:

Type Enforcement (TE)許可ルールが欠落している。

このアクセスを許可するためのロード可能モジュールを生成するには、次のコマンドを実行します。

```
> sudo audit2allow
```

具体的にどのルールによってアクセスが拒否されているかを確認するには、**audit2allow -a**を使用して、**audit.log**ファイルに記録されたすべてのイベントから強制ルールを表示するか、**audit2allow -i FILENAME**を使用して、特定のファイルに保存したメッセージについてルールを表示できます。

例 3: アクセスを拒否している行の表示

```
> sudo audit2allow -i testfile
#===== syslogd_t =====
allow syslogd_t apmd_log_t:file append;
```

mymoduleという名前のSELinuxモジュールを作成し、このモジュールをロードして以前に拒否されたアクセスを許可できるようにするには、次のコマンドを実行します。

```
> sudo audit2allow -a -R -M mymodule
```

audit.logファイルに記録されたすべてのイベントに対してこれを実行する場合は、**-a -M**コマンド引数を使用します。特定のファイルにある特定のメッセージのみに対してこれを実行するには、次の例のように**-i -M**を使用します。

例 4: 以前に拒否されたアクションを許可するポリシーモジュールの作成

```
> sudo audit2allow -i testfile -M example
***** IMPORTANT *****
To make this policy package active, execute:

semodule -i example.pp
```

audit2allowコマンドで示されているように、このモジュールを実行できるようになりました。実行するには、**semodule -i**コマンドに続けて、**audit2allow**によって作成されたモジュールの名前(上の例では**example.pp**)を使用します。

3 setroubleshootを使用したAVCメッセージの分析

使いやすい方法でAVC拒否メッセージを分析するには、setroubleshootツールを使用できます。

3.1 setroubleshootの概要

3.1.1 setroubleshootとは

setroubleshootは、カーネルからのSELinux監査イベントを収集し、これらのイベントを分析するツールです。このようなイベントが発生した場合、setroubleshootによって管理者に通知されます。

3.1.2 setroubleshootコンポーネント

SELinuxのトラブルシューティングプロセスには、以下のコンポーネントが必要です。これらのコンポーネントはすべてデフォルトでSLE Microにインストールされています。

- setroubleshoot-serverでは、次のツールを提供します。
 - setroubleshootd - 受信要求とプラグイン定義を処理するメインデーモン。このデーモンはオンデマンドで有効化されるため、systemdサービスを介して実行する必要はありません。特権ユーザと専用のsetroubleshootユーザのみが管理できます。
 - ファイル/var/lib/setroubleshoot/setroubleshoot_database.xml内のアラートのデータベース。
 - sealert - /var/log/audit.logを分析するためのコマンドラインユーザインタフェース。
 - sedispatch - SELinux AVCメッセージをスキャンし、DBusメッセージに変換してからデーモンに渡す監査ディスパッチャ。
- setroubleshoot-plugins - このプラグインは、AVCメッセージの分析に使用され、問題の解決方法に関する提案を提供します。

3.1.3 setroubleshootの動作

setroubleshootは、デーモンと分析プラグインで構成されます。プラグインが問題を検出すると、デーモンに問題が報告され、デーモンはこれが既知の問題であるかどうかを確認します。既知の問題ではない場合、新しい問題が、提案された解決策とともにデータベースに追加されます。

3.1.4 setroubleshootの利点

setroubleshootは、SELinuxでセキュリティ保護されたシステムの問題を解決するのに役立つ次の機能を備えています。

- AVC拒否がある場合に管理者にアラートを送信する。
- AVC拒否を自動的に分析する。
- システム設定の調整や更新のインストールなど、考えられる修正を提案する。
- 以前のアラートを参照する。

3.2 setroubleshootの構成

setroubleshootの設定を調整する必要はありませんが、デフォルト値の変更が必要な特定のユースケースに直面することがあります。以降のセクションでは、通常のユースケースについて説明します。

setroubleshootの設定ファイルは/etc/setroubleshootです。通常は、電子メール通知を設定する以外に設定を変更する必要はありません。ただし、設定を変更する必要がある場合は、このファイルを編集するか、**setroubleshootd**コマンドを使用して特定の項目を設定できます。コマンドの構文は次のとおりです。

```
# setroubleshootd -c  
SECTION.OPTION=VALUE
```

たとえば、`from_address`オプションを設定するには、このコマンドを次のように実行します。

```
# setroubleshootd -c  
email.from_address="example@mail.com"
```

3.2.1 **setroubleshoot**のログレベルの設定

デフォルトのログレベル(`sealert_log`と`setroubleshootd_log`の値)は`warning`に設定されています。ただし、この値を次のいずれかに設定できます。

critical

システムの機能を妨げる重大なエラーのみがログに記録されます。

error

システムに影響を及ぼす可能性のある重大なエラーが報告されます。

warning

予期しない症状が発生したり、近い将来に問題が発生する可能性があることを示します。ただし、システムは期待どおりに動作しています。

info

システムが正しく実行されていることの確認がログに記録されます。

debug

デバッグ用の詳細情報がログに記録されます。

3.2.2 電子メール通知を送信するための**setroubleshoot**の設定

システムでAVC拒否が発生している場合に、`setroubleshoot`から電子メール通知を送信できます。

これらの通知を受信するには、次の手順に従います。

1. `/etc/setroubleshoot/setroubleshoot.conf`を開きます。
2. このファイルで、次の設定項目をニーズに合わせて調整します。

smtp_host

SMTPサーバがローカルホスト上で実行されていない場合、SMTPサーバのアドレスを入力します。

smtp_port

デフォルトは25です。通常、この値を調整する必要はありません。

from_address

送信者のアドレスを追加します。

subject

すべてのメッセージの汎用の件名を設定します。

recipients_filepath

通知の受信者リストの場所を指定します。

use_sendmail

SendMailを使用する場合、trueに設定します。

3. メール受信者ファイルを、recipients_filepathオプションで定義したパスに作成します(デフォルトでは/var/lib/setroubleshoot/email_alerts-recipients)。
各電子メールアドレスは1行に1つずつ記述する必要があります。コメントは#記号で指定します。

3.2.3 setroubleshootデータベースの設定

setroubleshootdデータベースのレコード数、その場所、またはファイル名のプレフィクスを変更できます。

database_dir

データベースのXMLファイルが存在するディレクトリの絶対パスを指定します。

filename

データベースファイル名のカスタムプレフィクスを設定します。設定すると、ファイル名はFILENAME_PREFIX_database.xmlのようになります。

max_alerts

データベース内のレコードの最大数を定義します。レコード数が無制限の場合は、0を指定します。

max_alert_age

設定した制限より古いアラートはデータベースから削除されます。year、month、day、hour、minute、secondの各単位は複数形でも使用でき、複数の単位を使用できます。たとえば、3 weeks 2 daysは23日に相当します。空白のままにした場合、制限はありません。

3.2.4 リモートサーバから情報を収集するためのsetroubleshootの設定

SELinuxの監査データをリモートサーバから収集するようにsetroubleshootを設定できます。そのためには、アドレスリストを設定します。

[listen_for_client] address_list

サーバ側に設定します。

[client_connect_to] address_list

クライアント側に設定します。

リストのアドレスは次の形式です。

```
[{FAMILY}]ADDRESS[:PORT_NUMBER]
```

ここで、{FAMILY}は、{inet}または{unix}%{path}sです。アドレスファミリーがinetである場合は、オプションでポート番号を指定できます。それ以外の場合、ポート番号はdefault_port設定オプションで指定されたデフォルト値に設定されます。デフォルト値{unix}%{path}s hostnameは、ローカルのUnixドメインソケットをリスンすることを意味します。

3.3 /var/log/audit/audit.logの分析の実行

setroubleshootツールで監査ログファイルを分析できるようにするには、次のコマンドを実行します。

```
> sudo sealert -a /var/log/audit/audit.log
```

次の出力例では、SSHDサービスに割り当てられているポート値が2つあります。

```
100% done
found 1 alerts in /var/log/audit/audit.log
-----

SELinux is preventing sshd from name_bind access on the tcp_socket port 2222.

**** Plugin bind_ports (92.2 confidence) suggests ****

If you want to allow sshd to bind to network port 2222
Then you need to modify the port type.
Do
# semanage port -a -t PORT_TYPE -p tcp 2222 ①
   where PORT_TYPE is one of the following: ssh_port_t, vnc_port_t, xserver_port_t.

**** Plugin catchall_boolean (7.83 confidence) suggests ****

If you want to allow nis to enabled
Then you must tell SELinux about this by enabling the 'nis_enabled' boolean.

Do
```

```
setsebool -P nis_enabled 1

**** Plugin catchall (1.41 confidence) suggests ****

If you believe that sshd should be allowed name_bind access on the port 2222 tcp_socket by
default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# ausearch -c 'sshd' --raw | audit2allow -M my-sshd
# semodule -X 300 -i my-sshd.pp

Additional Information:
...

First Seen                2024-02-07 14:26:27 UTC
Last Seen                 2024-02-08 03:30:12 UTC
Local ID                  b5cbdd75-3f8d-425d-af75-f6cbf1540ffd

Raw Audit Messages
type=AVC msg=audit(1707363012.797:25): avc: denied { name_bind } for
pid=841 comm="sshd" src=2222 scontext=system_u:system_r:sshd_t:s0-s0:c0.c1023
tcontext=system_u:object_r:unreserved_port_t:s0 tclass=tcp_socket permissive=0

Hash: sshd,sshd_t,unreserved_port_t,tcp_socket,name_bind
```

- 1 bind_ports プラグインにより、この問題に最適な解決策が提供されます。

4 法的事項

Copyright © 2006–2025 SUSE LLC and contributors. All rights reserved.

この文書は、GNUフリー文書ライセンスのバージョン1.2または(オプションとして)バージョン1.3の条項に従って、複製、頒布、および/または変更が許可されています。ただし、この著作権表示およびライセンスは変更せずに記載すること。ライセンスバージョン1.2のコピーは、「GNUフリー文書ライセンス」セクションに含まれています。

SUSEの商標については、<https://www.suse.com/company/legal/> を参照してください。その他の第三者のすべての商標は、各社の所有に帰属します。商標記号(®、™など)は、SUSEおよび関連会社の商標を示します。アスタリスク(*)は、第三者の商標を示します。

本書のすべての情報は、細心の注意を払って編集されています。しかし、このことは正確性を完全に保証するものではありません。SUSE LLC、その関係者、著者、翻訳者のいずれも誤りまたはその結果に対して一切責任を負いかねます。

A GNUフリー文書利用許諾契約書(GFDL)

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. この使用許諾書を一字一句そのままの複製および頒布することは許可されますが、変更は許可されません。

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材料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する利用許諾通告を、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材料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。