SELinux

概要

このトピックでは、Security-Enhanced Linuxに関する基本情報を提供します。

目的

SELinux、およびSLE MicroにSELinuxを設定する方法を理解する必要があります。

所要時間

この記事の理解には40分ほどを要します。

発行日: 11/12/2025

目次

1 SELinuxについて 2

2 SELinuxの入手 2

3 SELinuxのモード 2

4 SELinuxのセキュリティコンテキスト 5

5 SELinuxポリシーの概要 7

6 SELinuxのブール値 9

7 SELinuxを管理するためのツール 11

8 法的事項 20

A GNUフリー文書利用許諾契約書(GFDL) 21

1 SELinuxについて

SELinuxは、そのセキュリティフレームワークをLinuxカーネルで使用する追加のLinuxセキュリティソリューションとして開発されました。その目的は、標準の任意アクセス制御(DAC)や、所有者/グループ/ワールド、読み込み/書き込み/実行という従来のファイル許可を超えた、よりきめ細かいセキュリティポリシーを実現することにありました。

SELinuxでは、オブジェクト(たとえば、ファイルやネットワークソケット)に付けられたラベルを用い、そのラベルを使用してアクセスを決定します。

SELinuxのデフォルトの動作は、あらゆるアクセスを拒否することです。SELinuxでは、SELinuxポリシーで特別に許可されたアクションのみが許可されます。SELinuxのもう1つのセキュリティ強化機能として、SELinuxでは、プロセスが同じシステムの他のプロセスのファイルにアクセスできなくなるまで、プロセスを厳密に制限できます。

SELinuxは、既存のセキュリティソリューションを置き換えるのではなく強化するために設計されました。たとえば、システムでSELinuxを使用していても、任意アクセス制御(DAC)は引き続き適用されます。アクセスが先にDACで拒否された場合、SELinuxは使用されません。そのアクセスはすでに別のメカニズムによってブロックされているからです。

2 SELinuxの入手

SELinuxは、SLE Microのインストール時にYaSTによってデフォルトでインストールされるか、または事前構築のイメージに含まれています。

SELinuxがシステムにセットアップされていない場合は、次のコマンドを実行します。

```
# transactional-update setup-selinux
```

コマンドが完了したら、システムを再起動します。このコマンドは、SELinuxポリシーがインストールされていなければインストールし、SELinuxの`enforcing`モードを設定して、`initrd`を再構築します。

3 SELinuxのモード

SELinuxは、`disabled`、`permissive`、または`enforcing`の3つのモードのいずれかで実行できます。

`disabled`モードを使用するということは、SELinuxポリシーのルールが一切適用されず、システムが保護されないことを意味します。したがって、`disabled`モードの使用はお勧めしません。

permissiveモードでは、SELinuxがアクティブになり、セキュリティポリシーがロードされてファイルシステムがラベル付けされ、アクセス拒否エントリがログに記録されます。ただし、ポリシーは強制されないため、アクセスは実際には拒否されません。

enforcedモードでは、セキュリティポリシーが適用されます。ポリシーで明示的に許可されていないアクセスはそれぞれ拒否されます。

SELinuxのモードの切り替えについては、3.1項「SELinuxモードの変更」を参照してください。

3.1 SELinuxモードの変更

SELinuxのモードを一時的または永続的に切り替えることができます。

3.1.1 SELinuxモードの一時的な変更

SELinuxをpermissiveまたはenforcingに一時的に設定するには、**setenforce**コマンドを使用します。

setenforceコマンドの構文は次のとおりです。

```
# setenforceMODE_ID
```

ここで、MODE_IDは、permissiveモードの場合は0、enforcedモードの場合は1です。

setenforceコマンドを使用してSELinuxを無効にすることはできないことに注意してください。

3.1.2 SELinuxモードの永続的な変更

SELinuxのモードを変更してシステムの再起動後もそのモードを維持するには、/etc/selinux/config設定ファイルを編集します。このファイルで、システムのSELinuxを無効にすることもできます。ただし、この操作はお勧めできません。SELinuxが原因でシステムに問題が発生している可能性がある場合は、代わりにpermissiveモードに切り替えてシステムをデバッグします。

/etc/selinux/configファイルで、SELINUXの値を次のようにdisabled、permissive、またはenforcedに変更します。

```
SELINUX=disabled
```

このファイルでの変更は、次回の再起動後に適用されます。

注記: disabledモードから切り替えた後のシステムの再ラベル付け

システムでSELinuxを無効にしてから、後で有効にする場合は、必ずシステムを再ラベル付けしてください。SELinuxが無効になっているときにファイルシステムに変更を加えた場合、その変更はコンテキストに反映されません(たとえば、新しいファイルにはコンテキストがありません)。したがって、システムを再ラベル付けする必要があります。そのためには、**restorecon**コマンドを使用するか、autorelabelブートパラメータを使用するか、または次回のブート時に再ラベル付けをトリガするファイルを作成します。ファイルを作成するには、次のコマンドを実行します。

```
# touch /etc/selinux/.autorelabel
```

再起動後に、/etc/selinux/.autorelabelファイルは別のフラグファイル/etc/selinux/.relabelledに置き換えられ、それ以降の再起動時に再ラベル付けされなくなります。

3.1.3 SELinuxのアクティブなモードの確認

モードを確認するには、次のコマンドを実行します。

```
# getenforce
```

このコマンドは、指定したMODE_IDに応じて、permissiveまたはenforcedを返します。

3.2 SELinuxが機能していることの確認

設定の変更を行う場合は、permissiveモードに切り替えると便利な場合があります。このモードの間に、ユーザがファイルに誤ってラベル付けしたために、enforcingモードに戻したときに問題が発生する可能性があります。

システムをセキュリティ保護された状態に戻すには、次の手順を実行します。

1. セキュリティコンテキストをリセットします。

   ```
   > sudo restorecon -R /
   ```

2. /etc/selinux/configにSELINUX=enforcingを設定して、enforcingモードに切り替えます。

3. システムを再起動し、再度ログインします。
4. `sestatus -v`コマンドを実行します。次のような出力が表示されるはずです。

```
> sudosestatus -v
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     requested(insecure)
Max kernel policy version:      33

Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_tty_device_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                       system_u:object_r:shell_exec_t:s0 \
                                -> system_u:object_r:shell_exec_t:s0
/bin/login                      system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 \
                                -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                    system_u:object_r:bin_t:s0 \
                                -> system_u:object_r:getty_exec_t:s0
/sbin/init                      system_u:object_r:bin_t:s0 -> \
                                system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                  system_u:object_r:sshd_exec_t:s0
```

5. システムが適切に機能していない場合は、`/var/log/audit/audit.log`のログファイルを確認してください。詳細については、SELinux troubleshooting (https://documentation.suse.com/smart-supported.html)を参照してください。

4 SELinuxのセキュリティコンテキスト

セキュリティコンテキストは、ファイルまたはプロセスに割り当てられる一連の情報です。セキュリティコンテキストは、SELinuxユーザ、役割、タイプ、レベル、およびカテゴリで構成されます。この情報を使用してアクセス制御が判断されます。

SELinuxユーザ

特定の一連の役割および特定の「レベル」の範囲に対して権限が付与される、ポリシーで定義されたID。各Linuxユーザは1人のSELinuxユーザにのみマップされます。ただし、1人のSELinuxユーザは複数の役割を持つことができます。
SELinuxは、Linuxが`/etc/passwd`で管理しているユーザアカウントのリストを使用せず、SELinux専用のデータベースとマッピングを使用します。規則により、ID名の末尾には`_u`が付きます。たとえば、`user_u`のようになります。
新しいLinuxアカウントを作成し、そのアカウントにSELinuxユーザを割り当てないと、デフォルトのSELinuxユーザが使用されます。通常、デフォルト値は`unconfined_u`です。デフォルト値の変更手順については、7.5.2項 「**`semanage login`コマンド**」を参照してください。

role

ユーザに付与できる許可のセットを定義します。役割では、この役割に割り当てられたユーザがアクセスできる「タイプ」を定義します。規則により、役割名の末尾には`_r`が付きます。たとえば、`system_r`のようになります。

type

タイプは、特定のファイルとプロセスがどのように相互作用できるかに関する情報を伝えます。プロセスは、具体的なSELinuxタイプを持つファイルで構成され、このタイプ以外のファイルにはアクセスできません。規則により、タイプ名の末尾には`_t`が付きます。たとえば、`var_t`のようになります。

level

マルチレベルセキュリティにおけるクリアランスレベルの範囲を指定するオプションの属性です。

category

プロセス、ファイル、およびユーザにカテゴリを追加できるオプションの属性です。
ユーザは同じカテゴリを持つファイルにアクセスできます。

SELinuxのコンテキストの例を次に示します。

```
allow user_t bin_t:file {read execute gettattr};
```

このルールの例では、コンテキストタイプ`user_t`を持つユーザ(このユーザはソースオブジェクトと呼ばれる)に対し、許可`read`、`execute`、および`getattr`を使用して、コンテキストタイプ`bin_t`を持つクラス**file**のオブジェクト(ターゲット)にアクセスすることを許可するように指定しています。

5 SELinuxポリシーの概要

ポリシーはSELinuxの重要な要素です。SELinuxポリシーは、どのオブジェクトがシステム上のどのファイル、ディレクトリ、ポート、およびプロセスにアクセスできるかを指定するルールを定義します。これを行うため、これらすべてに対してセキュリティコンテキストが定義されます。

SELinuxポリシーには膨大な数のルールが含まれます。管理しやすくするために、ポリシーは多くの場合、モジュールに分割されます。これにより、管理者はシステムの部分ごとに保護のオン/オフを切り替えることができます。

システムのポリシーを編集する場合、モジュール形式のポリシーを使用するか、モノリシックなポリシーを使用するかを選択できます。後者では1つの巨大なポリシーを使用してシステム上のすべてを保護します。モノリシックなポリシーではなく、モジュール形式のポリシーを使用することを強くお勧めします。モジュール形式のポリシーの方がはるかに管理が容易です。

SLE Microには、SELinuxポリシー`targeted`が付属します。

5.1 SELinuxのモジュールの使用

管理者は、モジュールのオン/オフを切り替えることができます。これは一部のSELinuxポリシーのみを無効にしたい場合や、特定のサービスをSELinuxによる保護なしでは実行しない場合に役立ちます。

使用中のすべてのSELinuxポリシーモジュールを表示するには、次のコマンドを実行します。

```
        semodule -l
```

オフに切り替えるモジュールの名前を取得してから、次のコマンドを実行します。

```
> sudo semodule -d MODULENAME
```

ポリシーモジュールをオンに切り替えるには、次のコマンドを実行します。

```
> sudo semodule -e MODULENAME
```

5.2 コンテナのポリシーの作成

SLE Microに付属するポリシーでは、コンテナがコンテナデータの外部にあるファイルにアクセスすることは、デフォルトでは許可されません。一方、ネットワークアクセスはすべて許可されます。通常、コンテナはバインドマウントで作成され、`/home`や`/var`などの他のディレクトリにアクセスできる必要があります。これらのディレクトリへのアクセスを許可したり、

逆にシステムでSELinuxを使用していても、一部のポートをコンテナに制限したりしたい場合があります。この場合、アクセスを有効または無効にする新しいポリシールールを作成する必要があります。SLE Microでは、この目的のためにUdicaツールが提供されています。

次の手順では、コンテナのカスタムポリシーを作成する方法を説明します。

1. SELinuxがenforcingモードになっていることを確認します。詳細については、3.1項「SELinuxモードの変更」を参照してください。

2. 次のパラメータを使用してコンテナを起動します。

```
# podman run -v /home:/home:rw -v /var/:/var/:rw -p 21:21 -it sle15 bash
```

   このコンテナは、マウントポイントへのアクセスを許可しない一方で、他のポートは制限しないデフォルトポリシーで実行されます。

3. コンテナを終了できます。

4. コンテナIDを取得します。

```
# podman ps -a

CONTAINER ID  IMAGE
             COMMAND     CREATED        STATUS            PORTS               NAMES
e59f9d0f86f2  registry.opensuse.org/devel/bci/tumbleweed/containerfile/opensuse/
bci/ruby:latest  /bin/bash   8 minutes ago  Up 8 seconds ago  0.0.0.0:21->21/tcp
 zen_ramanujan
```

5. Udicaがコンテナのカスタムポリシーを作成するために使用するJSONファイルを作成します。

```
# podman inspect e59f9d0f86f2 >OUTPUT_JSON_FILE
```

   たとえば、`OUTPUT_JSON_FILE`を`container.json`に置き換えます。

6. Udicaを実行し、コンテナパラメータに従ってポリシーを生成します。

```
# udica -jOUTPUT_JSON_FILECUSTOM_CONTAINER_POLICY
```

   次に例を示します。

```
# udica -j container.json custom_policy
```

7. 提供される指示に従い、次のコマンドを実行してポリシーモジュールをロードします。

```
# semodule -i custom_policy.cil /usr/share/udica/templates/
{base_container.cil,net_container.cil,home_container.cil}
```

8. 次のように`--security-opt`オプションを使用して、コンテナを新しいポリシーモジュールで実行します。

```
# podman run --security-opt label=type:custom_policy.process -v /home:/home:rw -v /
var/:/var/:rw -p 21:21 -it sle15 bash
```

6 SELinuxのブール値

SELinuxのブール値を使用することで、ポリシーを柔軟に管理できます。たとえば、ブール値を使用すると、あるサーバで特定のポリシーを無効にし、別のサーバでは同じポリシーをアクティブにしたままにすることができます。つまり、ブール値はポリシールールのスイッチとして理解できます。特定のポリシーを変更するのではなく、オフに切り替えることができます。ポリシーコードでは、ブール値は「チューナブル」と呼ばれます。ブール値はポリシーに含まれているため、ポリシーをロードするとすぐに利用できます。

ブール値は、永続的に変更することも、一時的に変更してセッションが終了するまで継続させることもできます。

SELinuxでは、ブール値の一覧と詳細の表示や、ブール値の状態の変更が可能なツールが提供されています。詳細については、次のセクションを参照してください。

6.1 ブール値の操作

6.1.1 ブール値の一覧

`getsebool`コマンドまたは**`semanage`**コマンドを使用して、現在定義されているブール値を一覧にできます。現在定義されているすべてのブール値と、その状態を一覧にするには、次のコマンドを実行します。

```
# getsebool -a

abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
...
```

特定のブール値の詳細を取得するには、**`semanage`**コマンドを次のように使用できます。

```
# semanage boolean -l
```

```
SELinux boolean                State   Default     Description

abrt_anon_write                (off  ,  off)       Allow abrt to anon write
abrt_handle_event              (off  ,  off)       Allow abrt to handle event
abrt_upload_watch_anon_write   (on   ,   on)       Allow abrt to upload watch anon write
```

個々のブール値のステータスを取得するには、次のコマンドを使用できます。

```
# getseboolBOOLEAN_NAME
```

または、単に**semanage boolean**の出力で**grep**コマンドを使用することもできます。

```
# semanage boolean -l | grepBOOLEAN_NAME
```

6.1.2 ブール値の切り替え

コマンド**setsebool**と**semanage**を使用してブール値を切り替えることができます。ブール値のステータスは、永続的に変更することも、セッション終了まで一時的に変更することもできます。ブール値を一時的に変更するには、次のコマンドを実行します。

```
# setseboolBOOLEAN_NAMEBOOLEAN_VALUE
```

ここで、BOOLEAN_VALUEは、onまたはoffのいずれかです。

ブール値を永続的に変更するには、次の2つのコマンドのいずれかを実行します。

```
# setsebool -PBOOLEAN_NAMEBOOLEAN_VALUE
```

または、**semanage**コマンドを使用します。

```
# semanage boolean -m --BOOLEAN_VALUEBOOLEAN_NAME
```

ここで、BOOLEAN_VALUEは、onまたはoffのいずれかです。

1つのブール値で複数のポリシールールを有効または無効にできます。どのポリシールールがどのブール値によって有効または無効にされているかを確認するには、ポリシーファイルを解析できる**sedispol**ツールを使用します。

```
# sedispol /etc/selinux/targeted/policy/policy.32
```

ポリシールールは通常、巨大であるため、fを選択してファイル名を指定し、出力ファイルを設定することをお勧めします。ファイル名を指定した後で、6を押します。これでそのファイルを検査できます。

7 SELinuxを管理するためのツール

SLE Microでは、システム上のSELinuxを管理するためのツールが提供されています。以下で説明するツールがシステムにインストールされていない場合は、次のコマンドを実行してインストールします。

```
# transactional-update pkg install policycoreutils-python-utils
```

正常にインストールされたら、システムを再起動します。

7.1 Zオプションの使用

SELinuxがインストールおよび設定されている場合は、**ls**、**id**、**ps**などの通常のコマンドで-Zを使用できます。このオプションを使用すると、ファイルやプロセスのセキュリティコンテキストを表示できます。たとえば、**ls**コマンドで使用すると、次のようになります。

```
> ls -Z /etc/shadow

        system_u:object_r:shadow_t:s0 /etc/shadow
```

7.2 chconコマンド

コマンド名**chcon**は、change context(コンテキストの変更)を表します。このコマンドは、ファイルの完全なセキュリティコンテキストをCLIで指定した値に変更したり、コンテキストの一部を変更したりできます。また、参照として機能するファイルを指定することもできます。

ファイルの完全なセキュリティコンテキストを変更する場合、コマンド構文は次のようになります。

```
# chconSECURITY_CONTEXTFILENAME
```

各要素の説明

- SECURITY_CONTEXTの形式は、SELinux_USER:ROLE:TYPE:LEVEL:CATEGORYです。たとえば、**system_u:object_r:httpd_config_t:s0**のようにコンテキストを指定できます。
- FILENAMEは、変更するコンテキストが含まれるファイルのパスです。

参照として機能する指定ファイルに従ってセキュリティコンテキストを設定するには、**chcon**を次のように実行します。

```
# chcon --reference=REFERENCE_FILEFILENAME
```

各要素の説明

- REFERENCE_FILEは、参照として使用するファイルのパスです。
- FILENAMEは、変更するコンテキストが含まれるファイルのパスです。

また、セキュリティコンテキストの一部のみを変更することもできます。**chcon**コマンドの一般的な構文は次のとおりです。

```
# chconCONTEXT_OPTIONCONTEXT_PARTFILENAME
```

オプションと引数には次の意味があります。

- コンテキストの部分によって、CONTEXT_OPTIONは次のいずれかになります。

  -u **resp** --user
  : 指定したファイルでSELinuxユーザコンテキストを変更するように指定します。

    ```
    # chcon -u system_u logind.conf
    ```

  -r **resp** --role
  : 指定したファイルのコンテキストで役割の部分のみを変更します。

    ```
    # chcon -r object_r logind.conf
    ```

  -t **resp** --type
  : 指定したファイルのコンテキストでタイプの部分のみを変更します。

    ```
    # chcon -t etc_t logind.conf
    ```

  -l **resp** --range
  : セキュリティコンテキストの範囲の部分のみを変更します。

    ```
    # chcon -l s0 logind.conf
    ```

- CONTEXT_PARTは、設定するセキュリティコンテキストの特定の値です。
- FILENAMEは、変更するコンテキストが含まれるファイルのパスです。

注記: シンボリックリンクでのchconの使用

デフォルトでは、シンボリックリンクのセキュリティコンテキストを変更した場合、リンクターゲットのコンテキストが変更され、シンボリックリンクのコンテキストは変更「されません」。**chcon**でリンクターゲットではなくシンボリックリンクのコンテキストを強制的に変更するには、次に示すように`--no-dereference`オプションを使用します。

```
# chcon --no-dereference -u system_u -t etc_t network.conf
```

再帰オプションを使用すると、ディレクトリ内のすべてのファイルのコンテキストを変更できます。

```
# chcon --recursive  system_u:object_r:httpd_config_t:s0 conf.d
```

7.3 getenforceコマンドおよびsetenforceコマンド

getenforceコマンドは、SELinuxの現在のモード(`Enforcing`、`Permissive`、または`Disabled`)を返します。

```
# getenforce

Permissive
```

setenforceコマンドは、SELinuxのモードを一時的にenforcingまたはpermissiveに変更します。このコマンドを使用してSELinuxを無効にすることはできません。変更は次回の再起動までしか持続しないことに注意してください。状態を永続的に変更するには、3.1項「SELinuxモードの変更」の説明に従ってください。

```
# setenforceMODE_ID
```

ここで、`MODE_ID`は、`permissive`モードの場合は`0`、`enforced`モードの場合は`1`です。

7.4 fixfilesスクリプト

このスクリプトでは、セキュリティコンテキストで次のタスクを実行できます。

- コンテキストが正しいかどうかを確認する
- 間違ったファイルコンテキストラベルを変更する
- 新しいポリシーを追加した場合にシステムに再ラベル付けする

スクリプトの構文は次のとおりです。

```
# fixfiles [OPTIONS] ARGUMENT
```

各要素の説明

- `OPTIONS`には以下を指定できます。

  `-l LOGFILE`
  : 指定したファイルに出力を保存します。

  `-o OUTPUT_FILE`
  : 指定した出力ファイルに、ファイルコンテキストがデフォルトとは異なるすべてのファイルの名前を保存します。

  `-F`
  : コンテキストのリセットを強制します。

- `ARGUMENT`は、次のいずれかになります。

  `check`
  : 間違ったラベルの以前のファイルコンテキストと現在のファイルコンテキストを表示します。変更は行いません。

  `relabel`
  : 現在ロードされているポリシーに従って、間違ったファイルコンテキストを再ラベル付けします。

  `restore`
  : 間違ったファイルコンテキストをデフォルト値に戻します。

  `verify`
  : 間違ったファイルコンテキストラベルを含むすべてのファイルを一覧にします。変更は行いません。

7.5 semanageコマンド

semanageコマンドを使用すると、ポリシーの一部を設定できます。ポリシーをソースから再コンパイルする必要はありません。このコマンドでは、次のタスクを実行できます。

- boolean引数を使用してブール値を管理するブール値の詳細については、6.1項「ブール値の操作」を参照してください。
- fcontext引数を使用してファイルのコンテキストを調整する
- login引数を使用してユーザマッピングを管理する
- user引数を使用してSELinuxユーザを管理する
- module引数を使用してSELinuxポリシーモジュールを管理する

コマンドの一般的な構文は次のとおりです。

```
# semanageARGUMENTOPTIONS [OBJECT_NAME]
```

各要素の説明

- ARGUMENTは、**login**、**user**、**fcontext**、**boolean**、**module**のいずれかです。
- OPTIONSは、指定したARGUMENTによって異なります。共通オプションについては、共通オプションに記載されています。
- OBJECT_NAMEは、指定したARGUMENTに応じて、ログイン名、モジュール名、ファイル名、またはSELinuxユーザのいずれかになります。

共通オプション

`-a`、`--add`
: 指定したオブジェクトを追加します。

`-h`、`--help`
: コマンドのヘルプを出力します。

--extract
: システムを変更するために使用されたコマンドを表示します(ブール値、ファイルコンテキストなど)。

`-l`、`--list`
: すべてのオブジェクトを一覧にします。

`-m`、`--modify`
: 指定したオブジェクトを変更します。

`-n`、`--noheading`
: 見出しを省略することでリスト操作の出力を変更します。

`-s`、`--seuser`
: SELinuxユーザを指定します。

その他のオプションは、特定の**`semanage`**コマンドに固有であり、対応するセクションで説明されています。

7.5.1 `semanage fcontext`コマンド

`semanage fcontext`コマンドを使用して、次のタスクを実行できます。

- ファイルコンテキストの定義を問い合わせる
- ファイルにコンテキストを追加する
- 独自のルールを追加する

`semanage fcontext`コマンドを使用してファイルコンテキストに対して変更を実行した場合、ポリシーの変更や再コンパイルは必要ありません。
共通オプションで説明されている共通オプションに加えて、**`semanage fcontext`**コマンドには次のオプションも指定できます。

`-e`、`--equal`
: このオプションを使用すると、指定したパスコンテキストのコンテキストを使用して、別のディレクトリ(指定されたターゲットパス)にあるファイルをラベル付けできます。たとえば、`/home`と同じコンテキストを別のホームディレクトリ`/export/home`に割り当てたい場合があります。このオプションを使用する場合は、ソースパスとターゲットパスを指定する必要があります。

```
# semanage fcontext -a -e /home /export/home
```

`-f`、`--ftype`
: ファイルタイプを指定します。次のいずれかの値を使用します。

  - `a` - すべてのファイル(デフォルト値でもあります)
  - `b` - ブロックデバイス

- `c` - キャラクタデバイス
- `d` - ディレクトリ
- `f` - 通常のファイル
- `l` - シンボリックリンク
- `p` - 名前付きパイプ
- `s` - ソケット

7.5.2 `semanage login`コマンド

`semanage login`では、次のタスクを実行できます。

- Linuxユーザを特定のSELinuxユーザにマップする。たとえば、Linuxユーザ**tux**を`sysadm_u`にマッピングするには、次のコマンドを実行します。

```
# semanage login -a -s sysadm_u tux
```

- Linuxユーザのグループを特定のSELinuxユーザにマップする。たとえば、**writers**グループのユーザを`user_u`にマッピングするには、次のコマンドを実行します。

```
# semanage login -a -s user_u %writers
```

このグループが、%の文字をプレフィクスとして**`semanage login -l`**の出力に一覧にされます。
ユーザグループはプライマリである必要があることに注意してください。SELinuxユーザを補助グループにマップすると、マッピングに互換性がなくなる可能性があるためです。

```
# semanage login -m -s staff_u %writers
```

- Linuxユーザを特定のSELinux MLS/MCSセキュリティ範囲にマップする。
- 作成済みのマッピングを変更する。このためには、前のコマンドの`-a`オプションを`-m`に置き換えるだけです。
- 新しいLinuxユーザに対してデフォルトのSELinuxユーザを設定する。通常のデフォルトのSELinuxユーザは`unconfined_u`です。この値を`staff_u`に変更するには、次のコマンドを実行します。

```
# semanage login -m -s staff_u __default__
```

7.5.3 semanage booleanコマンド

semanage booleanコマンドは、SELinuxポリシーのブール値を制御する場合に使用します。コマンドの概要は次のとおりです。

```
semanage boolean [-h] [-n]  [ --extract |
       --deleteall | --list [-C] | --modify ( --on | --off | -1 | -0 ) boolean ]
```

共通オプションに加えて、**semanage boolean**コマンド専用の次のオプションを使用できます。

--list -C
: ブール値のローカル変更のリストを表示します。

-m --on | -1
: 指定したブール値をオンに切り替えます。

-m --off | -0
: 指定したブール値をオフに切り替えます。

-D、--deleteall
: ブール値のすべてのローカル変更を削除します。

このコマンドの最も一般的な使用法は、特定のブール値のオン/オフを切り替えることです。たとえば、ブール値`authlogin_yubikey`をオンに切り替えるには、次のコマンドを実行します。

```
# semanage boolean -m on authlogin_yubikey
```

7.5.4 semanage userコマンド

semanage userコマンドは、SELinuxユーザと、役割およびMLS/MCSレベルとの間のマッピングを制御します。

共通オプションで説明されている共通オプションに加えて、**semanage use**コマンドには次のオプションも指定できます。

-R [ROLES]、--roles [ROLES]
: SELinuxの役割のリスト。複数の役割を二重引用符で囲んでスペースで区切るか、`-R`を複数回使用できます。

このコマンドを使用して、次のタスクを実行することができます。

- 次のコマンドを実行して、役割へのSELinuxユーザのマッピングを一覧にする。

```
# semanage user -l
```

- user_u SELinuxユーザに割り当てられた役割を変更する。

```
# semanage user -m -R "system_r unconfined_r user_r"
```

- admin_uに役割staff_rとカテゴリs0を割り当てる。

```
# semanage user -a -R "staff_r -r s0 admin_u
```

- 新しいSELinuxユーザを作成する。たとえば、staff_rの役割を持つadmin_uを作成します。-Pを使用して、このユーザのラベル付けのプレフィクスを定義する必要もあります。

```
# semanage user -a -R "staff_r" -P admin admin_u
```

7.5.5 semanage moduleコマンド

semanage moduleコマンドでは、SELinuxポリシーモジュールをインストール、削除、無効化、または有効化できます。

共通オプションで説明されている共通オプションに加えて、**semanage fcontext**コマンドには次のオプションも指定できます。

-d、--disable
: 指定したSELinuxポリシーモジュールを無効化します。

```
# semanage module --disable MODULE_NAME
```

-e、--enable
: 指定したSELinuxポリシーモジュールを有効化します。

```
# semanage module --enable MODULE_NAME
```

7.6 sestatusコマンド

sestatusは、SELinuxが実行されているシステムのステータスを取得します。

コマンドの一般的な構文は次のとおりです。

```
sestatus [OPTION]
```

オプションと引数を指定せずにこのコマンドを実行すると、次の情報が出力されます。

```
# sestatus

SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     requested (insecure)
Max kernel policy version:      33
```

このコマンドには次のオプションを指定できます。

-b

システムのブール値のステータスを表示します。

-v

`/etc/sestatus.conf`ファイルに一覧にされているファイルとプロセスのセキュリティコンテキストを表示します。

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。