Linux セキュリティ フルエディション 完全性検査ご利用ガイド

はじめに

本書では、「エフセキュア Linux セキュリティ フルエディション 」の完全性検査の利用方法について説明します。

1. 用語についての説明

完全性検査の機能で使用される用語について以下に説明します。

既知のファイル: 完全性検査の対象となっているファイルのことです。デフォルトで/bin の下のファイルなどが登録されています。
ベースライン: 改ざんの有無を判定する基準となる情報で、ハッシュ値、タイムスタンプ、パーミッションなどをまとめたものです。パスワードにより保護されています。

2. GUI からの操作

完全性検査の機能は、GUI の「詳細設定モード」から、「完全性検査」の項目で設定/変更が可能です。

サブ項目の「既知のファイル」で、既知のファイルの一覧の確認と、追加/削除が行えます。

新たに既知のファイルを追加する場合、「追加するファイルのフルパス」、「保護設定」、「アクション設定」、「対象外の属性」を設定します。

「保護設定」、「アクション設定」、「対象外の属性」の各設定値の意味は以下の通りです。

保護設定: **監視** : ファイルを監視します。ファイルは変更可能です。
保護 : ファイルに対する変更をすべて拒否します。ファイルを開くことはできますが、変更することはできません。

アクション設定: **許可**: 変更されたファイルが実行または開いたときのアクセスを許可します。
拒否: 変更されたファイルのアクセスを拒否します。変更されたファイルは開くことも、実行することもできません。

対象外の属性: **モード**: 権限の変更を対象外にします。
ユーザ: 所有者の変更を対象外にします。
グループ: グループの変更を対象外にします。
サイズ: ファイルサイズの変更を対象外にします。
更新時間: 更新日時の変更を対象外にします。
ハッシュ: ファイル内容の変更を対象外にします

注 1）通常、ファイルの内容が変更された際にはファイルの更新日時とサイズも変わるため、ハッシュ属性のみ対象外にすることは推奨されません。
注 2）WebUI から追加した既知のファイルは、警告送信が無効に設定されます。警告送信を行いたい場合は、後述のコマンドラインからの操作を行ってください。

既知のファイルを追加した場合、あるいは既存の既知のファイルを変更した場合、ベースラインを作成する必要があります。

ベースラインを作成するファイルを既知のファイルから選択し、「選択したファイルのベースラインを更新する」をクリックします。

変更されたファイルが多数になる場合は、サブ項目の「ベースラインの作成」から、全ての既知のファイルのベースラインを更新することが可能です。

3. コマンドラインからの操作

コマンドラインでの完全性検査の操作は、/opt/f-secure/fsav/bin/fsic を使用して行います。
詳細な使用方法については、”-h”オプションをつけてコマンドを実行しご確認ください。
ここでは代表的な使い方について紹介します。

既知のファイルの追加は、”-a” オプションを使用して行います。
例）/var/www/test.html と/usr/bin/hoge を既知のファイルに追加する場合
fsic -a /var/www/test.html /usr/bin/hoge

この際に、保護設定、アクション設定、対象外の属性、警告送信をオプションで指定できます。
保護設定: “--protect={yes,no}”のオプション: yes に設定すると保護設定が「保護」に設定されます。 no 場合、「監視」に設定されます。
アクション設定: “--access={allow,deny}”: deny に設定すると「拒否」に設定されます。
allow の場合、「許可」に設定されます。
対象外の属性: “--ignore={hash,mtime,mode,uid,gid,size}: 指定した項目が対象外に設定されます。
hash=ハッシュ、mtime=更新時間、mode=モード、uid=ユーザ、gid=グループ、size=サイズをそれぞれ意味します。
警告設定: “--alert={yes,no}”: 変更が行われた場合に、セキュリティ警告のイベントを作成するかどうかの設定です。no に設定するとセキュリティ警告が作成されません。yes の場合、警告設定が有効になります。

例）/var/www/index.html と/bin/huga を保護設定=監視、アクション=許可、対象外の属性=ユーザ、グループ、警告設定=有効で追加する場合
fsic -a --protect=no --access=allow --ignore=uid,gid --alert=yes /var/www/index.html /bin/huga

追加あるいは変更したファイルのベースラインの作成は、”-b”オプションで行います。

例）/var/www/test.html と/usr/bin/hoge のベースラインを更新する場合
fsic -b /var/www/test.html /usr/bin/hoge

全ての既知のファイルのベースラインを更新する場合、”-B”オプションで行います。
fsic -B

ベースライン更新時には、パスワードを入力する必要があります。

4. コマンドラインの応用

コマンドラインで操作する場合の、応用的な使い方を幾つか紹介します。
例 1）特定のディレクトリの下のファイルを全て既知のファイルに追加する方法
ここでは/opt/f-secure/fsav 以下のファイルを全て追加する方法を例示します。

```
# find /opt/f-secure/fsav -type f | xargs fsic –a
```

（必要に応じて-a の後に監視設定やアクション設定などのオプションを追加できます）

例 2）ベースラインの作成時のパスワード入力を自動で行う方法
以下のようなシェルを作成し、引数でパスワードを記入したファイルを指定します。

```
#!/bin/sh

file=$1

if [ ! -r $file ]; then
        echo "Passphrase file $file does not exists or is not readable"
        exit 1
fi

passphrase=`cat $file`

if [ -z "$passphrase" ]; then
        echo "Failed to read passphrase from $file"
        exit 1
fi

fsic -B << EOF
$passphrase
$passphrase
EOF
```

5. ソフトウェアインストールモードについて

既知のファイルで保護設定を「保護」にしているファイルを変更する場合、あるいは、保護設定が「監視」であっても変更時のエラーを抑制したい場合、ソフトウェアインストールモードがご利用頂けます。

ソフトウェアインストールモードを WebUI から利用する場合、以下の手順になります。

1. ウェブインターフェースを開きます。
2. 「一般タスク」ページに移動します。
3. 「ソフトウェアのインストール」を選択します。
4. ソフトウェアインストールモードウィザードから、ベースラインのパスワードを入力して次へ進みます。
5. 検査が完了するまで待ち、次へ進みます。
6. ソフトウェアインストールモードになるので、必要なプログラムのアップデートを行ってください。
7. インストール後、ベースラインのパスワードを設定し、次へ進んでください。
8. 新しいベースラインが作成されます。

以上で作業は完了です。

コマンドラインから行う場合、fsims がご利用頂けます。
以下のコマンドでソフトウェアインストールモードが有効になります。
/opt/f-secure/fsav/bin/fsims on

以下のコマンドでソフトウェアインストールモードが無効になり、ベースラインが再作成されます。新しいパスワードを入力してください。
/opt/f-secure/fsav/bin/fsims off

●免責

本書に記載された内容は、情報の提供だけを目的としています。したがって本書を用いた運用は必ずお客様自身の責任と判断により行ってください。これらの情報の運用の結果についてはエフセキュア株式会社はいかなる責任も負いません。本書の作成にあたっては細心の注意を払っていますが、記述に誤りや欠落があってもエフセキュア株式会社はいかなる責任も負わないものとします。

本書は 2014 年 7 月時点の情報を基に記述されており、ご利用時に変更されている場合もあります。

●商標

エフセキュア及び三角マークは、F-Secure Corporation の登録商標です。また、エフセキュアの製品名、マーク、ロゴは同社の商標または登録商標です。その他、記載されている、製品名、社名は各社の商標または登録商標です。

以上

2014 年 7 月
エフセキュア株式会社
プロダクトグループ
富安洋介