suEXEC サポート

suEXEC 機能により、Apache ユーザは Web サーバを実行しているユーザ ID とは 異なるユーザ ID で CGI プログラムや SSI プログラムを実行することができます。CGI プログラムまたは SSI プログラムを実行する場合、通常は web サーバと同じユーザで実行されます。

適切に使用すると、この機能によりユーザが個別の CGI や SSI プログラムを開発し実行することで生じるセキュリティ上の危険を、 かなり減らすことができます。しかし、suEXEC の設定が不適切だと、 多くの問題が生じ、あなたのコンピュータに新しいセキュリティホールを 作ってしまう可能性があります。あなたが root に setuid されたプログラムと、それらから生じるセキュリティ上の問題の管理に 詳しくないようなら、suEXEC の使用を検討しないように強く推奨します。

トピック

始める前に

この文書の先頭に飛ぶ前に、Apache グループとこの文書での仮定を知っておくべきでしょう。

第 1 に、あなたが setuid と setgid 操作が可能な UNIX 由来のオペレーティングシステムを使っていることを想定しています。 これは、すべてのコマンド例にあてはまります。その他のプラットホームでは、もし suEXEC がサポートされていたとしても設定は異なるかもしれません。

第 2 に、あなたが使用中のコンピュータの セキュリティに関する基本的な概念と、それらの管理について詳しいことを 想定しています。これは、setuid/setgid 操作、あなたのシステム上でのその操作による様々な効果、 セキュリティレベルについてあなたが理解しているということを含みます。

第 3 に、改造されていない suEXEC コードの使用を想定しています。suEXEC のコードは、多くのベータテスタだけでなく、開発者によっても注意深く精査され テストされています。それらの注意により、簡潔で信頼できる安全な コードの基盤が保証されます。このコードを改変することで、 予期されない問題や新しいセキュリティ上の危険が生じることがあります。 セキュリティプログラミングの詳細に通じていて、 今後の検討のために成果を Apache グループと共有しようと思うのでなければ、suEXEC コードは変えないことを 強く推奨します。

第 4 に、これが最後ですが、suEXEC を Apache のデフォルトインストールには含めないことが Apache グループで決定されています。これは、suEXEC の設定には管理者の詳細にわたる慎重な注意が必要だからです。 suEXEC の様々な設定について検討が終われば、管理者は suEXEC を通常のインストール方法でインストールすることができます。 これらの設定値は、suEXEC 機能の使用中にシステムセキュリティを適切に保つために、 管理者によって

慎重に決定され指定されることが必要です。 この詳細な手順により、Apache グループは、suEXEC のインストールについて、注意深く十分に検討してそれを使用することを 決定した場合に限っていただきたいと考えています。

それでも進みますか? よろしい。では、先へ進みましょう!

suEXEC セキュリティモデル

suEXEC の設定とインストールを始める前に、 まず実装しようとしているセキュリティモデルについて論じておきます。 それには、suEXEC の内部で行なわれていること、 システムのセキュリティを保証するために警告されることを よく理解しておいた方がよいでしょう。

suEXEC は、Apache web サーバから呼び出される setuid された "wrapper" プログラムが基本となっています。設計した CGI、または SSI プログラムへの HTTP リクエストがあると、この wrapper が呼び出されます。このようなリクエストがあると、Apache はそのプログラムが実行される際のプログラム名とユーザ ID とグループ ID を指定して suEXEC wrapper を実行します。

それから、wrapper は成功または失敗を決定するため 以下の処理を行ないます。これらの状態のうち一つでも失敗した場合、 プログラムは失敗をログに記録してエラーで終了します。 そうでなければ、後の処理が続けられます。

1. wrapper が適切な数の引数で呼び出されたか?
   wrapper は適切な数の引数が与えられた場合にのみ実行されます。 適切な引数のフォーマットは Apache Web サーバに解釈されます。 適切な数の引数を受け取らなければ、攻撃をされたか あなたの Apache バイナリの suEXEC の部分が どこかおかしい可能性があります。
2. wrapper を実行しているユーザはこのシステムの正当なユーザか?
   これは、wrapper を実行しているユーザが 本当にシステムの利用者であることを保証するためです。
3. この正当なユーザは wrapper の実行を許可されているか?
   このユーザは wrapper 実行を許可されたユーザですか? ただ一人のユーザ (Apache ユーザ) だけが、 このプログラムの実行を許可されます。
4. 対象のプログラムが安全でない階層の参照をしているか?
   対象のプログラムが '/' から始まる、または '..' による参照を行なっていますか? これらは許可されません。 対象のプログラムは Apache の web 空間内になければなりません。
5. 対象となるユーザ名は正当なものか?
   対象となるユーザ名は存在していますか?
6. 対象となるグループ名は正当なものか?
   対象となるグループ名は存在していますか?
7. 目的のユーザはスーパーユーザではないか?
   今のところ、suEXEC は 'root' による CGI/SSI プログラムの実行を許可していません。
8. 対象となるユーザ ID は、最小の ID 番号よりも大きいか?
   最小ユーザ ID 番号は設定時に指定されます。これは、 CGI/SSI プログラム実行を許

可されるユーザ ID のとりうる最小値です。これは "system" 用のアカウントを閉め出すのに有効です。

9. 対象となるグループはスーパーユーザのグループでは ないか?
今のところ、suEXEC は 'root' グループによる CGI/SSI プログラムの実行を許可していません。
10. 対象となるグループ ID は最小の ID 番号よりも大きいか?
最小グループ ID 番号は設定時に指定されます。これは、 CGI/SSI プログラム実行を許可されるグループ ID のとりうる最小値です。 これは "system" 用のグループを閉め出すのに有効です。
11. wrapper が正常に対象となるユーザとグループになれるか?
ここで、setuid と setgid の起動によりプログラムは対象となるユーザとグループになります。 グループアクセスリストは、 ユーザが属しているすべてのグループで初期化されます。
12. プログラムが置かれるディレクトリは存在しているか?
ディレクトリが存在しないなら、そのファイルも存在しないかもしれません。
13. ディレクトリが Apache のドキュメントツリー内にあるか?
リクエストがサーバ内のものであれば、 要求されたディレクトリがサーバのドキュメントルート配下にありますか? リクエストが UserDir のものであれば、 要求されたディレクトリがユーザのドキュメントルート配下にありますか?
14. ディレクトリを他のユーザが書き込めるようになって いないか?
ディレクトリを他ユーザに開放しないようにします。 所有ユーザだけがこのディレクトリの内容を改変できるようにします。
15. 対象となるプログラムは存在するか?
存在しなければ実行できません。
16. 対象となるプログラムファイルが他アカウントから 書き込めるようになっていないか?
所有者以外にはプログラムを変更する権限は与えられません。
17. 対象となるプログラムが setuid または setgid されていないか?
UID/GID を再度変更してのプログラム実行はしません
18. 対象となるユーザ/グループがプログラムの ユーザ/グループと同じか?
ユーザがそのファイルの所有者ですか?
19. 安全な動作を保証するための環境変数クリアが可能か?
suEXEC は、安全な環境変数のリスト (これらは設定時に作成されます) 内の変数として渡される安全な PATH 変数 (設定時に指定されます) を設定することで、 プロセスの環境変数をクリアします。
20. 対象となるプログラムを exec して実行できるか?
ここで suEXEC が終了し、対象となるプログラムが開始されます。

ここまでが suEXEC の wrapper におけるセキュリティモデルの標準的な動作です。もう少し厳重に CGI/SSI 設計についての新しい制限や規定を取り入れることもできますが、suEXEC はセキュリティに注意して慎重に少しずつ開発されてきました。

このセキュリティモデルを用いて サーバ設定時にどのように許すことを制限するか、また、suEXEC を適切に設定するとどのようなセキュリティ上の危険を避けられるかに 関するより詳しい情報については、"とかげに注意" (Beware the Jabberwock) の章を参照してください。

suEXEC の設定とインストール

ここから楽しくなります。

suEXEC 設定オプション

--enable-suexec
: このオプションは、デフォルトではインストールされず、 有効にはならない suEXEC 機能を有効にします。 suEXEC を使うように APACI に要求するには、--enable-suexec オプションにあわせて少なくとも一つは --with-suexec-xxxxx オプションが指定されなければなりません。

--with-suexec-bin=PATH
: セキュリティ上の理由により、suexec バイナリのパスはサーバに ハードコードされている必要があります。デフォルトのパスを 変えたいときはこのオプションを使ってください。例えば、 --with-suexec-bin=/usr/sbin/suexec のように。

--with-suexec-caller=UID
: Apache を通常動作させるユーザ名[1]を指定します。 このユーザだけが suexec の実行を許可されたユーザになります。

--with-suexec-userdir=DIR
: suEXEC がアクセスを許されるユーザホームディレクトリ配下の サブディレクトリを指定します。 このディレクトリ以下の全実行ファイルは、"安全な"プログラムになるよう、 suEXEC がそのユーザとして実行できるようにします。 "単純な" UserDir ディレクティブを使っている場合 (すなわち "*" を含まないもの)、これと同じ値を設定すべきです。 Userdir ディレクティブがそのユーザのパスワードファイル内の ホームディレクトリと同じ場所を指していなければ、 suEXEC は適切に動作しません。デフォルトは "public_html" です。
: 各 UserDir が異なった仮想ホストを設定している場合、 それらを全て一つの親ディレクトリに含めて、 その親ディレクトリの名前をここで指定する必要があります。このように指定されなければ "~userdir" cgi へのリクエストが動作しません。

--with-suexec-docroot=DIR
: Apache のドキュメントルートを設定します。これが suEXEC の動作で使用する唯一のディレクトリ階層になります (UserDir の指定は別)。デフォルトでは --datedir に "/htdocs" というサフィックスをつけたものです。 "--datadir=/home/apache" として設定すると、 suEXEC wrapper にとって "/home/apache/htdocs" がドキュメントルートとして使われます。

--with-suexec-uidmin=UID
: suEXEC の対象ユーザとして許される UID の最小値を指定します。 大抵のシステムでは 500 か 100 が一般的です。 デフォルト値は 100 です。

--with-suexec-gidmin=GID
: suEXEC の対象グループとして許される GID の最小値を指定します。大抵のシステムでは 100 が一般的なので、 デフォルト値としても 100 が使われています。

--with-suexec-logfile=FILE
: suEXEC の処理とエラーが記録されるファイル名を指定します。(監査やデバッグ目的に有用) デフォルトではログファイルは "suexec_log" という名前で、 標準のログファイルディレクトリ (--logfiledir) に置かれます。

--with-suexec-safepath=PATH

CGI 実行ファイルに渡される安全な PATH 環境変数です。 デフォルト値は "/usr/local/bin:/usr/bin:/bin" です。

suEXEC 設定の確認
suEXEC wrapper をコンパイルしてインストールする前に、設定内容を --layout オプションで確認できます。
出力例:

```
suEXEC setup:
suexec binary: /usr/local/apache/sbin/suexec
document root: /usr/local/apache/share/htdocs
userdir suffix: public_html
logfile: /usr/local/apache/var/log/suexec_log
safe path: /usr/local/bin:/usr/bin:/bin
caller ID: www
minimum user ID: 100
minimum group ID: 100
```

suEXEC wrapper のコンパイルとインストール
--enable-suexec オプションで suEXEC 機能を有効にすると、 "make" コマンドを実行した時に suEXEC のバイナリ (Apache 自体も) が自動的に作成されます。
すべての構成要素が作成されると、それらのインストールには "make install" コマンドが実行できます。バイナリイメージの "suexec" は --sbindir オプションで指定されたディレクトリにインストールされます。 デフォルトの場所は "/usr/local/apache/sbin/suexec" です。
インストール時には root 権限が必要なので注意してください。wrapper がユーザ ID を設定するために、所有者 root でのセットユーザ ID ビットをそのファイルのモードに設定しなければなりません。

suEXEC の有効化と無効化

起動時に、Apache は "sbin" ディレクトリで "suexec" を探します (デフォルトは "/usr/local/apache/sbin/suexec") 。 適切に設定された suEXEC がみつかると、 エラーログに以下のメッセージが出力されます。

```
[notice] suEXEC mechanism enabled (wrapper: /path/to/suexec)
```

サーバ起動時にこのメッセージが出ない場合、 大抵はサーバが想定した場所で wrapper プログラムが見つからなかったか、 setuid root としてインストールされていないかです。

suEXEC の仕組みを使用するのが初めてで、Apache が既に動作中であれば、 Apache を kill して、再起動しなければなりません。HUP シグナルや USR1 シグナルによる単純な再起動では不十分です。

suEXEC を無効にする場合は、"suexec" ファイルを削除してから Apache を kill して再起動します。

suEXEC の使用

仮想ホスト:
suEXEC wrapper の使い方として、 VirtualHost 設定での SuexecUserGroup ディレクティブを通したものがあります。 このディレクティブをメインサーバのユーザ ID と異なるものにすると、CGI リソースへのすべてのリクエストは、その <VirtualHost> で指定された User と Group として実行されます。<VirtualHost> でこのディレクティブが指定されていない場合、 メインサーバのユーザ ID が想定されます。

ユーザディレクトリ:
suEXEC wrapper は、リクエスト先のユーザとして CGI を実行するためにも使えます。これは期待する実行権限のユーザ ID の前に、"~" 文字を置くことで実現されます。 この機能を動作させるために必要なことは、CGI をそのユーザで実行できること、そのスクリプトが上記のセキュリティ検査をパスできることです。

suEXEC のデバッグ

suEXEC wrapper は、上記で述べた --with-suexec-logfile オプションで指定されたファイルにログ情報を記録します。 wrapper を適切に設定、インストールできていると思う場合、 どこで迷っているか見ようとするならこのログとサーバの エラーログを見るとよいでしょう。

とかげに注意: 警告と事例

注意! この章は完全ではありません。この章の最新改訂版については、 Apache グループのオンラインドキュメント[2]版を参照してください。

サーバの設定に制限をもうける wrapper について、 いくつか興味深い点があります。suEXEC に関する "バグ" を報告する前にこれらを確認してください。

- suEXEC の興味深い点
- 階層構造の制限

  セキュリティと効率の理由から、suEXEC の全てのリクエストは 仮想ホストへのリクエストにおける最上位のドキュメントルート内か、 ユーザディレクトリへのリクエストにおける個々のユーザの最上位の ドキュメントルート内に残らなければなりません。例えば、四つの仮想ホストを設定している場合、 仮想ホストの suEXEC に有利なように、メインの Apache ドキュメント階層の外側に全ての仮想ホストのドキュメントルートを 構築する必要があります。(例は後日記載)
- suEXEC の PATH 環境変数

  これを変更するのは危険です。この指定に含まれる各パスが 信頼できる ディレクトリであることを確認してください。 世界からのアクセスにより、誰かがホスト上でトロイの木馬 を実行できるようにはしたくないでしょう。
- suEXEC コードの改造

  繰り返しますが、何をやろうとしているか把握せずにこれをやると 大きな問題を引き起こしかねません。 可能な限り避けてください。

URI References

[1] http://httpd.apache.org/docs-2.1/mod/mpm_common.html#user
[2] http://httpd.apache.org/docs-2.1/suexec.html