Linux Security11.10 cmd edition fssp.conf デフォルトセッティング

Linux Security コマンドディションは「fssp.conf」値(※)で設定を行って頂いております。下記にLinux Security11.10のfssp.confのデフォルト値を掲載しておりますのでデフォルト値との差分確認にご利用ください。後継のLinux Security 64(LS64)はfssp.confで設定可能であった詳細な設定は用意されておらず、デフォルト設定で最適動作を行うようにセッティングされておりますので、特別な要件がない限り、LS64をデフォルト設定でご利用ください。

※こちらの設定値については詳細な解説ドキュメントを用意させいただいておりません。

```
[root@localhost fssp]# cat fssp.conf
#
# This is a configuration file for F-Secure Security Platform
#
# Copyright (c) F-Secure Corporation. All Rights Reserved.
#

#
# Specify whether the product should scan all files or only the files that
# match the extensions specified in the 'Extensions to Scan' setting.
#
# Possible values:
#   0 - All files
#   1 - Only files with specified extensions
#
odsFileScanFiles 0


#
# Specify the list of filename extensions to be scanned. You can also use
# wildcards: '?' matches exactly one character, '*' matches any number of
# characters, including zero (0) characters. '.' (a single dot), if given
# alone, matches files without extension. The matching is case-insensitive.
#
odsIncludedExtensions .,acm,app,arj,asd,asp,avb,ax,bat,bin,boo,bz2,cab,ceo,chm,cmd,cnv,com,cpl,csc,dat,dll,do?,drv,eml,exe,gz,hlp,hta,htm,html,htt,inf,ini,js,jse,lnk,lzh,map,mdb,mht,mif,mp?,msg,mso,nws,obd,obt,ocx,ov?,p?t,pci,pdf,pgm,pif,pot,pp?,prc,pwz,rar,rtf,sbf,scr,shb,shs,sys,tar,td0,tgz,tlb,tsp,tt6,vbe,vbs,vwp,vxd,wb?,wiz,wml,wpc,ws?,xl?,zip,zl?,{*


#
# Specify whether executables should be scanned. If a file has any
# user/group/other executable bits set, it is scanned regardless of the file
# extension.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsScanExecutables 0


#
# Determines whether some paths (either files or directories) will be excluded
# from scanning. Use full, absolute path name. Type each path on its own line.
# Path names may contain whitespaces.
#
odsFileExcludedPaths /proc¥n/sys


#
# Determines whether some files can be excluded from scanning. Please note
# that the files specified here are excluded from scanning even if they would
# be included in scanning according to what is defined in the other scanning
# settings
#
# Possible values:
#   0 - Disabled
#   1 - Enabled
#
odsFileEnableExcludedPaths 1



#
# Specifies whether archives should be scanned when a manual scan is launched.
# The supported archive formats include, for example, .tar.gz, .zip
#
# Possible values:
#   0 - Disabled
#   1 - Enabled
#
odsFileScanInsideArchives 1



#
# Defines how many levels deep to scan in nested archives. It is not
# recommended to set this value too high as this will make the product more
# vulnerable to DoS (Denial of Service) attacks. If an archive has more nested
# levels than the limit, a scan error is generated.
#
odsFileMaximumNestedArchives 5
```

```
#
# Define whether MIME encoded data should be scanned for malicious content.
# NOTE: Current MIME decoding support does not work for mail folders where
# multiple e-mail messages are stored in a single file, such as Netscape,
# Mozilla, Thunderbird, Evolution or mbox mail folders. MIME decoding only
# works if each e-mail message is stored as a separate file.
#
# Possible values:
#   0 - Disabled
#   1 - Enabled
#
odsFileScanInsideMIME 0


#
# Defines how password-protected archives should be handled. If set to Yes,
# password protected archives are considered to be safe and access is allowed.
# Otherwise access is not allowed.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsFileIgnorePasswordProtected 1


#
# Defines what happens when the first infection is found inside an archive. If
# set to 'Yes', scanning will stop on the first infection. Otherwise the whole
# archive is scanned.
#
```

```
# Possible values:
#   0 - No
#   1 - Yes
#
odsStopOnFirst 0



#
# Specify the primary action to take when an infection is detected.
#
# Possible values:
#   0 - Do nothing
#   1 - Report only
#   2 - Disinfect
#   3 - Rename
#   4 - Delete
#   5 - Abort scan
#   6 - Custom
#
odsFilePrimaryActionOnInfection 2



#
# If "Custom" is chosen as the primary action, the custom action must be
# specified here. Please note that the custom action will be executed as the
# super user of the system so consider and check carefully the command you
# specify. Custom action script or program receives one parameter, full
# pathname of the infected file.
#
odsFileCustomPrimaryAction
```

```
#
# Specify the secondary action to take when an infection is detected and the
# primary action has failed.
#
# Possible values:
#   0 - Do nothing
#   1 - Report only
#   2 - Disinfect
#   3 - Rename
#   4 - Delete
#   5 - Abort scan
#   6 - Custom
#
odsFileSecondaryActionOnInfection 3


#
# If "Custom" is chosen as the secondary action, the custom action must be
# specified here. Please note that the custom action will be executed as the
# super user of the system so consider and check carefully the command you
# specify. Custom action script or program receives one parameter, full
# pathname of the infected file.
#
odsFileCustomSecondaryAction


#
# Specify the primary action to take when suspected infection is detected.
#
# Possible values:
```

```
#   0 - Do nothing
#   1 - Report only
#   3 - Rename
#   4 - Delete
#
odsFilePrimaryActionOnSuspected 1


#
# Specify the secondary action to take when suspected infection is detected
# and the primary action has failed.
#
# Possible values:
#   0 - Do nothing
#   1 - Report only
#   3 - Rename
#   4 - Delete
#
odsFileSecondaryActionOnSuspected 0


#
# Set this on to report and handle riskware detections. Riskware is potential
# spyware.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsScanRiskware 1
```

```
#
# Type of riskware that should not be detected.
#
odsExcludedRiskware ;


#
# Specify the primary action to take when riskware is detected.
#
# Possible values:
#   0 - Do nothing
#   1 - Report only
#   3 - Rename
#   4 - Delete
#
odsFilePrimaryActionOnRiskware 1


#
# Specify the secondary action to take when riskware is detected and the
# primary action has failed.
#
# Possible values:
#   0 - Do nothing
#   1 - Report only
#   3 - Rename
#   4 - Delete
#
odsFileSecondaryActionOnRiskware 0
```

```
#
# Defines the upper limit for the time used for scanning a file (1 second
# resolution). A recommended upper limit would be, for example, 1 minute.
#
odsFileScanTimeout 60


#
# Specify the action to take after a scan timeout has occurred.
#
# Possible values:
#   0 - Report as Scan Error
#   2 - Report as Clean File
#
odsFileScanTimeoutAction 0


#
# Should actions be taken automatically or should user be prompted to confirm
# each action.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsAskQuestions 1


#
# Read files to scan from from standard input.
```

```
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsInput 0


#
# Print out all the files that are scanned, together with their status.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsList 0


#
# Should infected filenames be printed as they are or should potentially
# dangerous control and escape characters be removed.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsRaw 0


#
# In standalone mode a new fsavd daemon is launched for every client. Usually
# you do not want this because launching the daemon has considerable overhead.
#
# Possible values:
#   0 - No
#   1 - Yes
#   2 - Auto
#
odsStandalone 2


#
# If "No", fsav command line client does not follow symlinks. If "Yes",
# symlinks are followed. This affects e.g. scanning a directory containing
# symlinks pointing to files outside of the directory.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsFollowSymlinks 0


#
# If enabled, only infected filenames are reported.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsSilent 0
```

```
#
# If enabled, only infected filenames are reported.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsShort 0


#
# If this setting is on, file access times are not modified when they are
# scanned. If a file is modified due to disinfection, then both access and
# modify times will change.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsFilePreserveAccessTimes 0


#
# Specifies how MIME messages with broken attachments will be handled. If set
# to 'Yes', files for which MIME decoding fails will be considered safe. If
# set to no, an error will be generated.
#
# Possible values:
#   0 - No
#   1 - Yes
```

```
#
odsFileIgnoreMimeDecodeErrors 0


#
# Defines how partial MIME messages should be handled. If set to 'Yes',
# partial MIME messages are considered safe and access is allowed. Partial
# MIME messages cannot reliably be unpacked and scanned.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsFileIgnorePartialMime 0


#
# Defines how MIME messages with broken headers should be handled. If set to
# 'Yes', broken MIME headers will be considered safe and access is allowed. If
# set to 'No', an error will be generated.
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsFileIgnoreInvalidMimeHeaders 0


#
# Do not scan files equal or larger than 2 GB (2,147,483,648 bytes). If this
# option is not set an error will be reported for large files.
```

```
#
# Possible values:
#   0 - No
#   1 - Yes
#
odsFileSkipLarge 0



#
#
#
#
# If "On", the FS-Engine is used for scanning files. If "Off", FS-Engine is
# not used.
#
# Possible values:
#   0 - Off
#   1 - On
#
odsUseFSE 1



#
# If "On", the Aquarius scanning engine is used for scanning files. If "Off",
# Aquarius is not used.
#
# Possible values:
#   0 - Off
#   1 - On
#
odsUseAquarius 1
```

```
#
#
#
# Maximum size of MIME message. Files larger than this are not detected as
# MIME messages. Increasing this number will increase scan time of large
# files.
#
daemonMaxMimeMessageSize 10485760


#
# MIME recognition frame size specifies how many bytes are searched from
# beginning of file for MIME headers.
#
daemonMaxMimeRecognitionFrameSize 4096


#
#
# Use this setting to set custom settings for Aquarius engine. The settings
# are given in a semicolon separated list, for example:
#
daemonAquariusCustomSettings


#
# Archives smaller than this size (in megabytes), are decompressed in memory.
#
advMaxDecompressMemory 50
```

```
#
# Archives larger than previous setting and smaller than this size (in
# megabytes), are decompressed in a temporary file. Archives larger than this
# can still be scanned, but slowly.
#
advMaxDecompressFile 100


#
# Directory where temporary files are created, if they are needed.
#
advDirectoryForTempFiles /tmp


#
# Compressed files having uncompressed/compressed size ratio higher than this
# are considered "compression-bombs" and will not be scanned. They will
# generate a scan error.
#
advMaximumCompressionRatio 2000


#
# F-Secure Internal. Do not change. This is the directory where in-use
# databases are kept.
#
daemonDatabaseDirectory /var/opt/f-secure/fssp/databases
```

```
#
# F-Secure internal. Do not change. This is the directory into which new
# databases are stored before they are taken into use.
#
daemonUpdateDirectory /var/opt/f-secure/fssp/update


#
# F-Secure internal. Do not change. This is the directory from where scan
# engine libraries are loaded.
#
daemonEngineDirectory /opt/f-secure/fssp/lib


#
# If ″Yes″, fsavd writes a log file. If ″No″, no log file is written.
#
# Possible values:
#   0 - No
#   1 - Yes
#
daemonLogfileEnabled 0


#
# Log file location: stderr - write log to standard error stream syslog -
# write log to syslog facility Anything else is interpreted as a filename to
# write log into.
#
daemonLogfile syslog
```

```
#
# Maximum number of simultaneously running fsavd scanner processes. (min. 1,
# max. 100)
#
daemonMaxScanProcesses 4


#
# FSAV will add the current user-id to the path to make it possible for
# different users to run independent instances of the server.
#
daemonSocketPath /tmp/.fsav


#
# Octal number specifying the mode (permissions) of the daemon socket. See
# chmod(1) and chmod(2) unix manual pages.
#
daemonSocketMode 0600


#
# Login name of owner for path elements (socket and directories) created for
# socket path.
#
socketpathOwner root


#
# Name of group for path elements (socket and directories) created for socket
# path.
#
socketpathGroup fsc


#
# If fsavd has to create the directory for socket path, this is the mode
# (permissions) used for the created directory.
#
daemonDirectoryMode 3755


#
# Syslog facility to use when logging to syslog.
#
# Possible values:
#   auth, authpriv, cron, daemon, ftp, kern, lpr, mail, news, syslog, user, uucp, local0, local1, local2, local3, local4, local5, local6, local7 - auth, authpriv, cron, daemon, ftp, kern, lpr, mail, news, syslog, user, uucp, local0, local1, local2, local3, local4, local5, local6, local7
#
daemonSyslogFacility daemon


#
#
#
#
# The keycode entered during installation.
#
licenseNumber xxxx-xxxx-xxxx-xxxx-xxxx
```

```
#
# The complete path that tells where this product is installed in the
# filesystem.
#
installationDirectory /opt/f-secure/fssp


#
# Unix time() when installation done.
#
installationTimestamp 1623838593


#
# F-Secure internal. Do not change. Text to be printed every day during
# evaluation use.
#
naggingText EVALUATION VERSION - FULLY FUNCTIONAL - FREE TO USE FOR 30 DAYS.¥nTo purchase license, please check http://www.F-Secure.com¥n


#
# F-Secure internal. Do not change. Text to be printed when evaluation period
# has expired.
#
expiredText EVALUATION PERIOD EXPIRED¥nTo purchase license, please check http://www.F-Secure.com
```