



Dr.Web Server Security Suite Ver.10.1 簡易構築ガイド -Linux 用-

株式会社 Doctor Web Pacific

初版 : 2015/11/10

改訂 : 2016/07/04

目次

1. はじめに	3
1.1 ライセンス証書の受領	3
1.2 ライセンス証書に含まれる内容	3
2. 環境前提条件	3
3. 準備	4
3.1 インストール環境の確認	4
3.2 リポジトリ設定	4
3.2.1 Cent OS 系	4
3.2.2 Ubuntu 系	5
3.3 ファイル	5
4. インストール	6
4.1 リポジトリからのインストール	6
4.2 インストーラ(.run)からのインストール	9
5. ケーススタディ	13
5.1 設定の確認と変更	13
5.1.1 設定の確認	13
5.1.2 設定の変更	13
5.2 Archive ファイルのスキャン	13
5.3 Web インターフェース	14
5.4 ライセンス更新	14
5.4.1 コマンドラインからの更新	14
5.4.2 Web インターフェースからの更新	15
5.5 コマンドラインからのスキャンの実行等	16
5.6 samba との連携	18
5.6.1 samba との連携時の設定	18
5.6.2 samba バージョン 4.2.x 以降を使用する場合	18
5.7 ESS サーバとの接続	20
5.8 OS が起動しない場合の対処	22



この度は、株式会社 DoctorWebPacific の製品をご購入いただき、誠にありがとうございます。本ガイドは、初めて弊社製品をご利用いただくお客様向けに、Server Security Suite(以下 SSS)を簡潔に構築いただくための手順を説明する資料となります。なお、詳細な機能や操作の説明に関しましては、製品マニュアルをご参照ください。

1. はじめに

1.1 ライセンス証書の受領

ライセンス証書は、Doctor Web Pacific(以下、DWP)または、DWP パートナー企業より、電子メールか郵送もしくはその両方の方法で、お客様へ送付いたします。

1.2 ライセンス証書に含まれる内容

ライセンス証書には、以下のライセンスに関する情報が記載されておりますので、大切に保管してください。

- custmer(お客様情報)
- product(購入製品名)
- serial number(製品用キーコード)
- license term(ライセンス期間)
- protected objects (購入ライセンス数)

2. 環境前提条件

本書は、下記の環境で動作確認の上作成しております。

- OS
Cent OS 6.5 (64bit)、Cent OS 7.0 (64bit)、Ubuntu 14.10 (64bit)
- samba のバージョン
Cent OS 6.5 : 3.6.23
Cent OS 7.0 : 4.1.12
Ubuntu 14.10 : 4.1.11
- selinux
無効
- iptables(FireWall)
無効



3. 準備

3.1 インストール環境の確認

OS 毎に以下のパッケージがインストールされているか確認し、インストールされていない場合はインストールしてください。

➤ Cent OS 6.5

glibc.i686、glibc.x86_64、glibc-common.x86_64、nss-softoken-freebl.i686、nss-softoken-freebl.x86_64、perl

➤ Cent OS 7.0

glibc.i686、glibc.x86_64、glibc-common.x86_64、nss-softoken-freebl.i686、nss-softoken-freebl.x86_64、perl、perl-Data-Dumper、perl-Sys-Syslog

➤ Ubuntu 14.10

libc6-i386、libc6、perl

3.2 リポジトリ設定

SSS をリポジトリからインストール(yum や apt-get を用いてインストール)する場合、以下の設定を行なってください。

3.2.1 Cent OS 系

/etc/yum.repos.d/内に以下の内容を含むファイル(drweb.repo 等)を作成してください。

```
[drweb]
name=DrWeb - 10.1.0
baseurl=http://repo.drweb.com/drweb/el5/10.1.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://repo.drweb.com/drweb/drweb.key
```

※ 上記は、64bit OS での内容です。32bit OS については、マニュアルを参照してください。

3.2.2 Ubuntu 系

- 1) 以下のコマンドを実行し、キーの追加を実施してください。

```
$ wget http://repo.drweb.com/drweb/drweb.key
$ sudo apt-key add ./drweb.key
```

- 2) /etc/apt/sources.list に以下の内容を追加してください。

```
deb http://repo.drweb.com/drweb/debian 10.1.0 non-free
```

- 3) 以下のコマンドを実行してください。

```
$ sudo apt-get update
```

3.3 ファイル

以下のファイルを用意してください。キーファイルおよびインストーラの入手方法については、「Dr.Web ダウンロード&アクティベーションガイド」を参照してください。

尚、SSS をリポジトリからインストールする場合は、インストーラ(.run ファイル)のダウンロードは不要です。

➤ キーファイル等

drweb32.key もしくは agent.key を用意し、インストール対象のサーバにコピーしてください。

ESS サーバ(バージョン 10)の Agent として接続する場合は、当該サーバの drwcsd.pub ファイルを用意してください。

※ AV DESK サーバの Agent として接続することはできません。

➤ インストーラ

インストーラ(.run ファイル)を用意し、インストール対象のサーバにコピーしてください。

※ リポジトリからインストールする場合は、不要です。



4. インストール

4.1 リポジトリからのインストール

- 1) 以下のコマンドを実行し、SSS のインストールを実行します。

CentOS の場合

```
# yum install drweb-file-servers
```

Ubuntu の場合

```
$ sudo apt-get install drweb-file-servers
```

【注意】 Kernel バージョンが 2.6.37 より古い環境(CentOS 6.x 等)では、SpIDer Guard の起動時に OS の再起動が発生する場合があります。以下のコマンドを実行し、SpIDer Guard の起動を停止してください。
下記のサービスにて、CentOS 6.x や CentOS 5.x を使用している場合は、必ず実行してください。
GMO クラウド社： Altus Basic シリーズ、Altus Isolate シリーズ

```
# drweb-ctl cfset LinuxSpider.Start No
```

- 2) インストールが完了した後、キーファイル(drweb32.key もしくは agent.key)を/etc/opt/drweb.com/に drweb32.key としてコピーします。
- 3) samba との連携設定を行なうため、以下のスクリプトを実行します。

※ samba と連携させない場合は、3)から 9)および 13)の手順は実行する必要はありません。

CentOS の場合

```
# /opt/drweb.com/share/drweb-smbspider-modules/drweb_smbspider_configure.sh
```

Ubuntu の場合

```
$ sudo /opt/drweb.com/share/drweb-smbspider-modules/drweb_smbspider_configure.sh
```

- 4) 以下のメッセージが表示されたら、「yes」と入力し、「Enter」キーを押します。

```
Do you want your smb.conf to be patched now? (YES/no)
```

- 5) 以下のメッセージが表示されたら、「yes」と入力し、「Enter」キーを押します。

```
Is "/usr/sbin/smbd" the Samba daemon in use? (YES/no)
```

- 6) 以下のメッセージが表示されたら、保護の対象を入力し、「Enter」キーを押します。

※ 表示されているもの全てを選択する場合は「A」、それ以外は対象の数字を入力します。

```
Samba conf file: "/etc/samba/smb.conf"
```

```
Select SMB shares the smb spider will be connected to.
```

```
1) [ ] homes
```

```
2) [ ] printers
```

```
Enter directory number to toggle selection.
```

```
Enter A or All to select all directories.
```

```
Enter N or None to deselect all directories.
```

```
Enter 0, Q or Quit when done.
```

```
All values are case insensitive.
```

```
Select:
```

- 7) 6)で選択した内容が表示されたら、誤りがないか確認後、「0」と入力し、「Enter」キーを押します。

```
Samba conf file: "/etc/samba/smb.conf"
```

```
Select SMB shares the smb spider will be connected to.
```

```
1) [X] homes
```

```
2) [X] printers
```

```
Enter directory number to toggle selection.
```

```
Enter A or All to select all directories.
```

```
Enter N or None to deselect all directories.
```

```
Enter 0, Q or Quit when done.
```

```
All values are case insensitive.
```

```
Select:
```

- 8) 以下のメッセージが表示されたら、「yes」と入力し、「Enter」キーを押します。

```
Do you agree with these changes? (YES/no)
```



- 9) 以下のメッセージが表示されたことを確認します。

```
Configuration of drweb-smb spider is completed successfully.  
#
```

- 10) 以下のコマンドを実行し、2つのサービスを再起動します。

- CentOS 6.5

```
# /etc/init.d/drweb-configd restart  
# /etc/init.d/drweb-spider-kmod restart
```

※ drweb-spider-kmod はプロセスとしては起動しません。

- CentOS 7.0

```
# systemctl restart drweb-configd
```

- Ubuntu

```
$ sudo service drweb-configd restart
```

- 11) 以下のコマンドを実行し、ライセンスが正常に読み込まれているか確認します。

- CentOS

```
# cat /var/log/messages | grep "License"  
Nov 10 20:50:37 sss101 drweb-configd[3164]: License number <Key No.>, expires <ライ  
センス期限>
```

- Ubuntu

```
$ sudo cat /var/log/syslog | grep "License"  
Nov 10 20:50:37 sss101 drweb-configd[3164]: License number <Key No.>, expires <ライ  
センス期限>
```

- 12) 以下のコマンドを実行し、SpIDer Guard for NSSを停止します。

- CentOS

```
# drweb-ctl cfset NSS.Start No
```

- Ubuntu

```
$ sudo drweb-ctl cfset NSS.Start No
```

- 13) samba 関連のサービスを再起動します。

※ samba と連携させない場合は、実行する必要はありません。

※ 初期状態では、アーカイブファイルに対してスキャンは行われません。

4.2 インストーラ(.run)からのインストール

- 1) インストーラ(.run ファイル)のパーミッションを変更し、実行権を付与します。

```
# chmod +x <インストーラ名>
```

- 2) 以下のコマンドを実行します。

➤ CentOS

```
# ./<インストーラ名>
```

➤ Ubuntu

```
$ sudo ./<インストーラ名>
```

※ ファイルの解凍が始まります。

- 3) 以下のメッセージが表示されたら、「yes」と入力し、「Enter」キーを押します。

```
This installation script will help you install Dr.Web for UNIX File Servers  
Do you want to continue? (YES/no)
```

- 4) 以下のメッセージが表示されたら、「1」と入力し、「Enter」キーを押します。

```
Select the installation type:  
1      Dr.Web for UNIX File Servers  
2      Custom Configuration  
  
Choose one configuration to install [1] :
```

- 5) 以下のメッセージが表示されたら、「yes」と入力し、「Enter」キーを押します。

```
Do you agree with the terms of this license? (yes/NO)
```

- 6) 以下のメッセージが表示されたら、「yes」と入力し、「Enter」キーを押します。

※ samba と連携させない場合は、「no」と入力し、「Enter」キーを押します。7)から 12)の手順は表示されません。

```
This installation script will help you to configure Dr.Web for UNIX File Servers  
Do you want to continue? (YES/no)
```

- 7) 以下のメッセージが表示されたら、「0」と入力し、「Enter」キーを押します。

```
Enter path to the Dr.Web license key file or '0' to skip:
```

- 8) 以下のメッセージが表示されたら、「yes」と入力し、「Enter」キーを押します。

```
Do you want your smb.conf to be patched now? (YES/no)
```

- 9) 以下のメッセージが表示されたら、「yes」と入力し、「Enter」キーを押します。

```
Is "/usr/sbin/smbd" the Samba daemon in use? (YES/no)
```

- 10) 以下のメッセージが表示されたら、保護の対象を入力し、「Enter」キーを押します。

※ 表示されているもの全てを選択する場合は「A」、それ以外は対象の数字を入力します。

```
Samba conf file: "/etc/samba/smb.conf"
```

```
Select SMB shares the smb spider will be connected to.
```

```
1) [ ] homes
```

```
2) [ ] printers
```

```
Enter directory number to toggle selection.
```

```
Enter A or All to select all directories.
```

```
Enter N or None to deselect all directories.
```

```
Enter 0, Q or Quit when done.
```

```
All values are case insensitive.
```

```
Select:
```

- 11) 10)で選択した内容が表示されたら、誤りがないか確認後、「0」と入力し、「Enter」キーを押します。

```
Samba conf file: "/etc/samba/smb.conf"
```

```
Select SMB shares the smb spider will be connected to.
```

```
1) [X] homes
```

```
2) [X] printers
```

```
Enter directory number to toggle selection.
```

```
Enter A or All to select all directories.
```

```
Enter N or None to deselect all directories.
```

```
Enter 0, Q or Quit when done.
```

```
All values are case insensitive.
```

```
Select:
```



- 12) 以下のメッセージが表示されたら、「yes」と入力し、「Enter」キーを押します。

```
Do you agree with these changes? (YES/no)
```

- 13) 以下のメッセージが表示されたら、「Yes」と入力し、「Enter」キーを押します。

```
Do you want to configure services? (YES/no)
```

- 14) 以下のメッセージが表示されたら、「Enter」キーを押します。

```
Press Enter to finish.
```

※ ESS サーバと接続させる場合は以降の手順は行わず、「5.5 ESS サーバとの接続」を参照してください。

- 15) Kernel バージョンが 2.6.37 より古い環境(CentOS 6.x 等)では、以下のコマンドを実行し、SpIDer Guard の起動を停止してください。

【注意】 Kernel バージョンが 2.6.37 より古い場合、SpIDer Guard の起動時に OS の再起動が発生する場合があります。その防止のため、SpIDer Guard の起動を停止します。

下記のサービスにて、CentOS 6.x や CentOS 5.x を使用している場合は、必ず実行してください。

GMO クラウド社 : Altus Basic シリーズ、Altus Isolate シリーズ

```
# drweb-ctl cfset LinuxSpider.Start No
```

- 16) キーファイル(drweb32.key もしくは agent.key)を/etc/opt/drweb.com/drweb32.key としてコピーします。

- 17) 以下のコマンドを実行し、2 つのサービスを再起動します。

➤ CentOS 6.5

```
# /etc/init.d/drweb-configd restart
# /etc/init.d/drweb-spider-kmod restart
```

※ drweb-spider-kmod はプロセスとしては起動しません。

➤ CentOS 7.0

```
# systemctl restart drweb-configd
```

➤ Ubuntu

```
$ sudo service drweb-configd restart
```

18) 以下のコマンドを実行し、ライセンスが正常に読み込まれているか確認します。

➤ CentOS

```
# cat /var/log/messages | grep "License"  
Nov 10 20:50:37 sss101 drweb-configd[3164]: License number <Key No.>, expires <ライ  
センス期限>
```

➤ Ubuntu

```
$ sudo cat /var/log/syslog | grep "License"  
Nov 10 20:50:37 sss101 drweb-configd[3164]: License number <Key No.>, expires <ライ  
センス期限>
```

19) 以下のコマンドを実行し、SpIDer Guard for NSS を停止します。

➤ CentOS

```
# drweb-ctl cfset NSS.Start No
```

➤ Ubuntu

```
$ sudo drweb-ctl cfset NSS.Start No
```

20) samba 関連のサービスを再起動します。

- ※ samba と連携させない場合は、実行する必要はありません。
- ※ 初期状態では、アーカイブファイルに対してスキャンは行われません。

5. ケーススタディ

【注意】本項のコマンド等の表記は、CentOS 6.5 の場合を記載しております。CentOS 7.0 や Ubuntu 14.10 の場合は、必要に応じて読み替えてください。

5.1. 設定の確認と変更

5.1.1 設定の確認

コマンドラインから以下のコマンドを実行すると、現在の設定が出力されます。

```
# drweb-ctl cfshow
```

※ 従来の INI ファイル形式で出力させる場合は、以下を実行してください。

```
# drweb-ctl cfshow --Ini
```

5.1.2 設定の変更

コマンドラインから以下のコマンドを実行することにより、設定を変更できます。

```
# drweb-ctl cfset <section>.<parameter> <設定値>
```

5.2. Archive ファイルのスキャン

初期状態では、アーカイブファイルのスキャンは無効になっています。有効にする場合は、以下のコマンドを実行してください。

```
# drweb-ctl cfset SMBSpider.ArchiveMaxLevel <最大ネストレベル>
# drweb-ctl cfset LinuxSpider.ArchiveMaxLevel <最大ネストレベル>
```

※ 最大ネストレベルを超えるアーカイブファイルに対してはスキャンは実行されません。

5.3. Web インターフェース

Web インターフェースを使用することにより、ステータスや検出された脅威の確認、設定の変更、ライセンスの更新を行なうことができます。

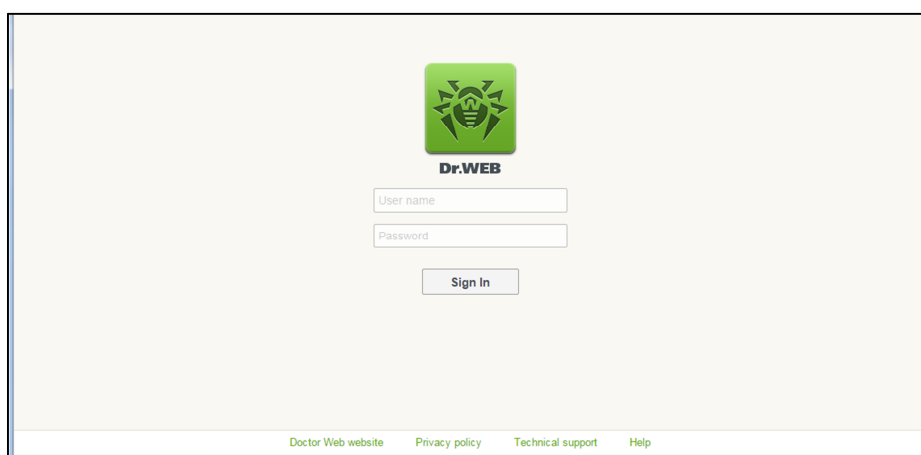
初期状態では、SSSをインストールしたサーバ上で以下の URL にアクセスすることにより、Web インターフェースを開くことができます。

URL : `https://127.0.0.1:4443/`

ID : `root`

Password : `root` のパスワード

※ 初期状態では、他の端末から Web インターフェースを開くことはできません。



※ 他の端末から Web インターフェースにアクセスできるようにする場合は、以下のコマンドを実行してください。

```
# drweb-ctl cfset HTTPD.ListenAddress <IP アドレス>:4443
```

5.4. ライセンス更新

5.4.1 コマンドラインからの更新

- 1) 新しいライセンスキー(drweb32.key もしくは agent.key)を/etc/opt/drweb.com/に drweb32.key としてコピーします。
- 2) 以下のサービスを再起動します。

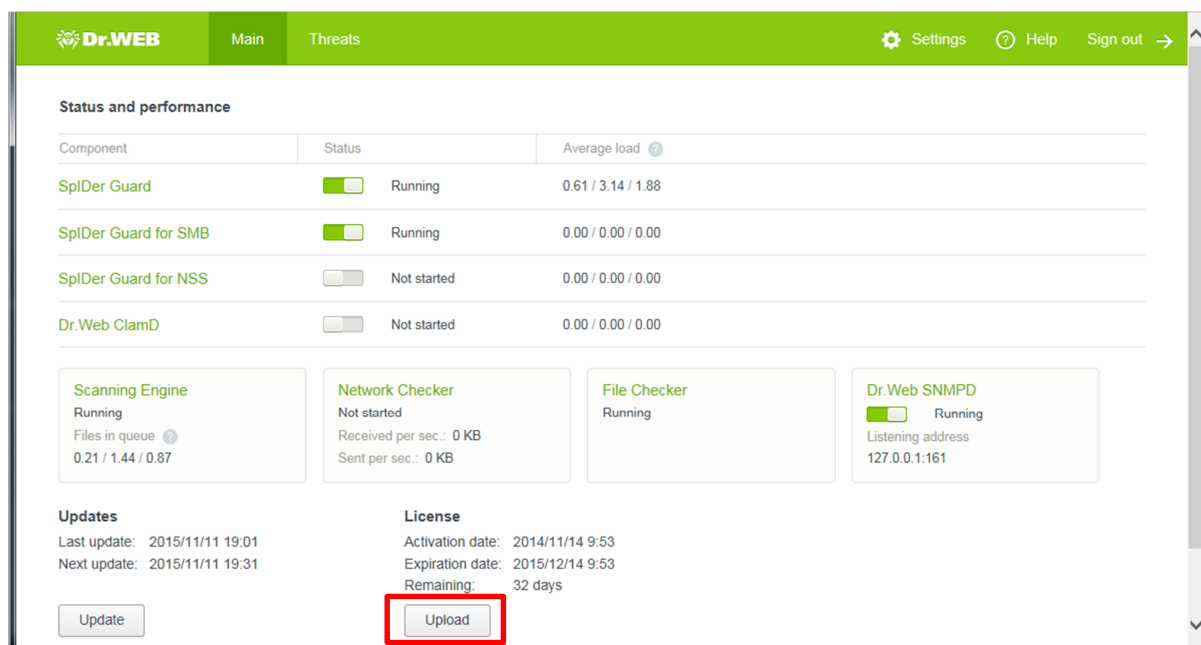
```
# /etc/init.d/drweb-configd restart
# /etc/init.d/drweb-spider-kmod restart
```

※ drweb-spider-kmod はプロセスとしては起動しません。

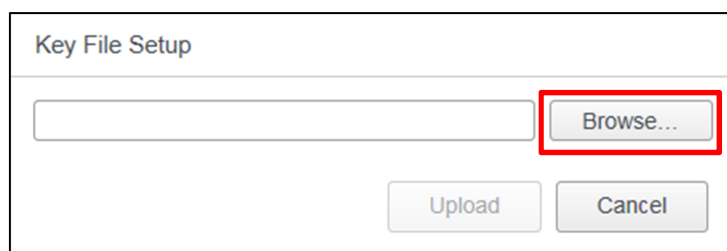
- 3) /var/log/messages を確認し、新しいライセンスに更新されたことを確認します。

5.4.2 Web インターフェースからの更新

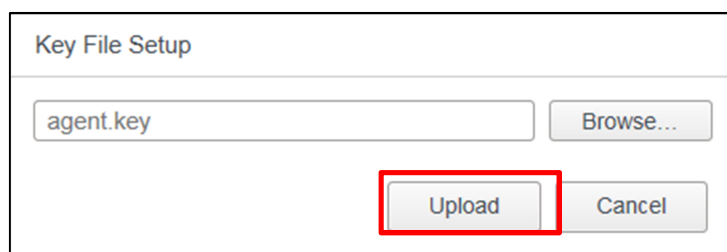
- 1) Web インターフェースにログインします。
- 2) [Main]メニュー内の License セクションの「Upload」ボタンをクリックします。



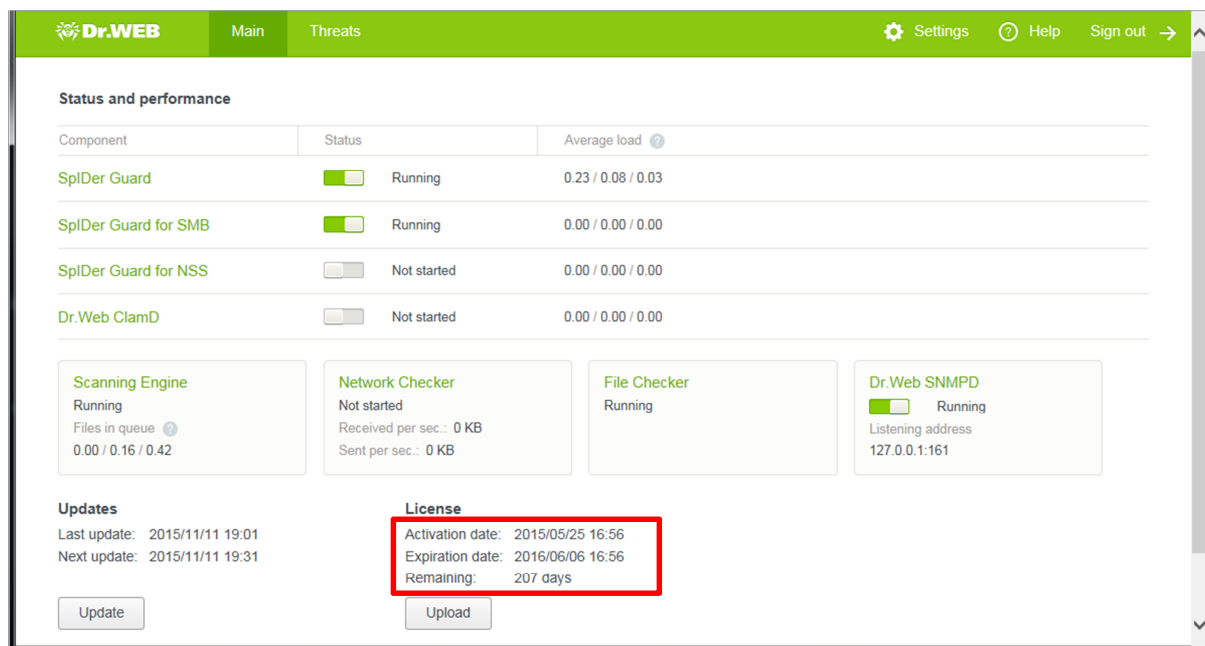
- 3) 「Browse」ボタンをクリックし、新しいライセンスキー(drweb32.key もしくは agent.key)を指定します。



- 4) 「Upload」ボタンをクリックします。



5) Web インターフェース上のライセンス情報が更新されたことを確認します。



6) /var/log/messages を確認し、新しいライセンスに更新されたことを確認します。

5.5. コマンドラインからのスキャンの実行等

※ 詳しくは、下記 URL を参照してください。

https://download.geo.drweb.com/pub/drweb/unix/server/10.0/documentation/html/en/dw_9_ctl_commandline.htm

1) コマンドラインからのスキャン

```
# drweb-ctl scan <スキャン対象のパス>
```

例) /home/test をスキャンする場合

```
# drweb-ctl scan /home/test
```

上記では、検出した脅威に対して隔離等はいきません。スキャンと同時に隔離を行なう場合は、下記となります。

```
# drweb-ctl scan --OnKnownVirus QUARANTINE <スキャン対象のパス>
```

2) 脅威を含むファイルの隔離

※ コマンドラインからのスキャンの際、隔離オプションを指定しなかった場合に実行してください。

※ drweb-configd が再起動されると、隔離等が行われていない脅威の情報はクリアされます。

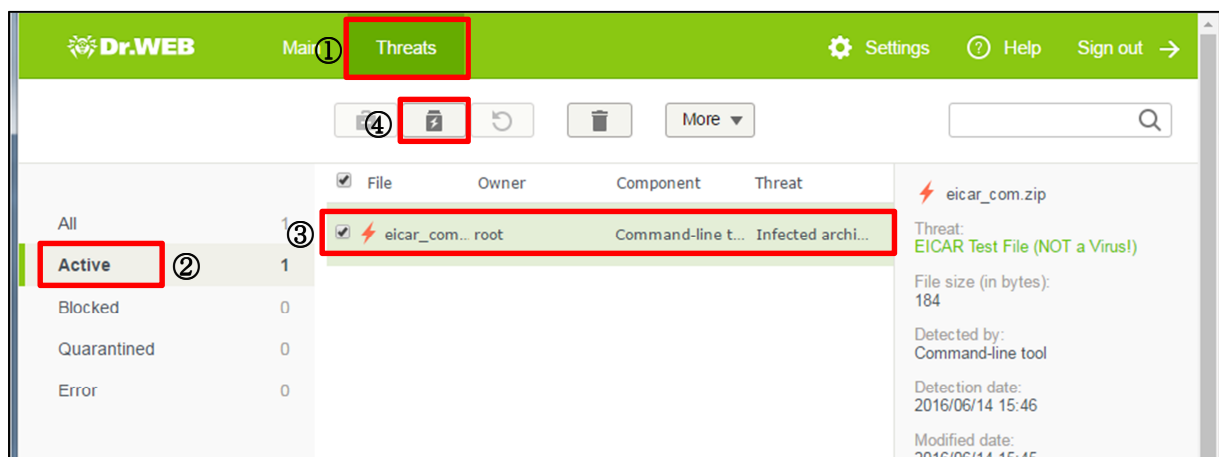
➤ コマンドラインから実行する場合

```
# drweb-ctl threats --Quarantine all
```


➤ Web インターフェースから実行する場合

Web インターフェースにログインし、「Threats」から「Active」をクリックすると、Dr.Web によって脅威が検出された隔離や削除が行われていないファイルの一覧が表示されます。

対象のファイルを選択し、「Move to quarantine」ボタンをクリックすると、隔離処理が行われます。



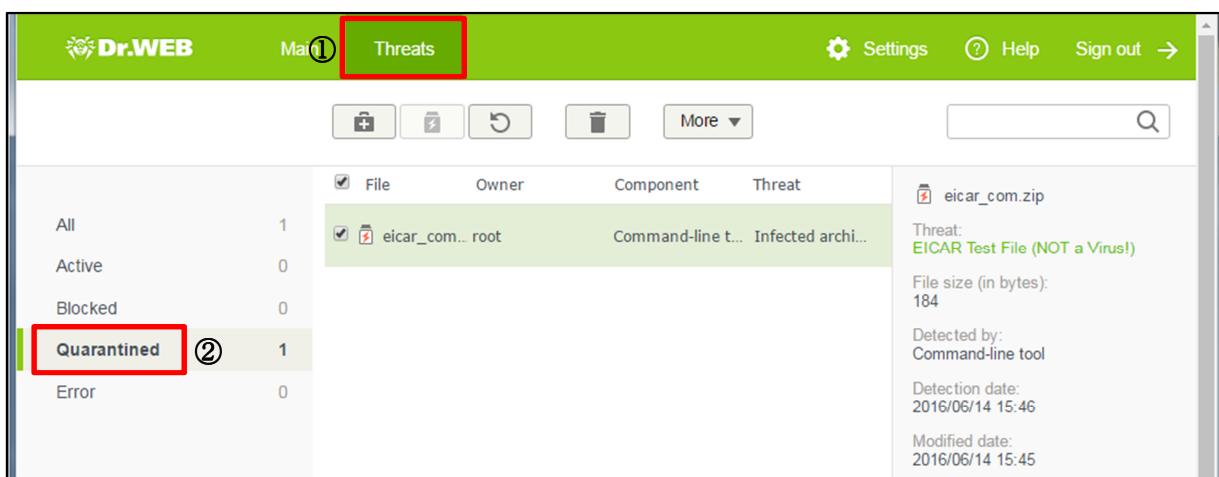
3) 隔離されたファイルの確認

➤ コマンドラインから実行する場合

```
# drweb-ctl quarantine
```

➤ Web インターフェースから実行する場合

Web インターフェースにログインし、「Threats」から「Quarantine」をクリックすると、隔離されているファイルを確認できます。





5.6. samba との連携

samba の共有フォルダへのスキャンは、SpIDer Guard for SMB によって実施されます。しかしながら、SpIDer Guard が起動している状態では、SpIDer Guard for SMB による処理が行われる前に SpIDer Guard による処理が実行されますので、ご注意ください。

※ SpIDer Guard が起動している場合には、すべての書き込みに対してスキャンが実施されます。

5.6.1 samba との連携時の設定

初期状態では、SpIDer Guard for SMB は、書き込み時にスキャンは実行しますが、脅威が検出された場合でも即時に隔離等は行わず、24 時間後(86400000ms)に隔離等を行います。また、脅威が検出された際には、<脅威が検出されたファイル名>.drweb.alert.txt というファイルが作成されます。

上記を踏まえ、必要に応じて、以下の項目については設定を変更してください。

コマンドラインでの parameter	Web インターフェースでの表示項目	初期値
AlertFiles ※警告ファイルの作成	Create a file describing the blocking reason	Yes
ActionDelay ※指定処理を行なうまでの待機時間	Delay before action	1d (86400000ms)
OnKnownVirus	Infected objects	Cure
OnIncurable	Curing errors	Quarantine
OnSuspicious	Suspicious	Quarantine
OnAdware	Adware	Pass
OnDialers	Dialers	Pass
OnJokes	Jokes	Pass
OnRiskware	Riskware	Pass
OnHacktools	Hacktools	Pass

※ コマンドラインにて指定する section は、全て SMBSpider です。

5.6.2 samba バージョン 4.2.x 以降を使用する場合

samba バージョン 4.2.x 以降を使用する場合、VFS SMB Module を作成する必要があります。

※ 4.1.x 以前については、予め用意されています。

詳しくは、下記をご確認ください。

https://download.geo.drweb.com/pub/drweb/unix/server/10.0/documentation/html/en/index.html?dw_9_app_g_compile_vfs.htm

- 1) 利用しているバージョンと同じバージョンの samba のソースコードを入手し、ビルドしてください。

入手したソースコードを用いて、configure と make を実行してください。



- 2) VFS SMB Module 作成用ソースコードを入手します。

Dr.Web のリポジトリより VFS SMB Module 作成用ソースコードを入手してください。

```
# yum install drweb-smbspider-modules-src
```

※ 上記を実行すると、/usr/src/に drweb-smbspider-10.1.0.src.tar.gz というファイルが作成されます。

- 3) VFS SMB Module 作成用ソースコードを展開し、ビルドします。

```
# tar -xzf drweb-smbspider-10.1.0.src.tar.gz
# cd ./drweb-smbspider-10.1
# ./configure --with-samba-source=<path_to_dir_with_Samba_src> && make
```

例) samba のソースコードがあるフォルダが/home/test/SOURCES/samba-4.2.10 の場合

```
# ./configure --with-samba-source=/home/test/SOURCES/samba-4.2.10 && make
```

- 4) 作成された VFS SMB Module を/usr/lib64/samba/vfs/にコピーします。

ビルド完了後、ビルドを実行したフォルダ内の.libs/フォルダに libsmb_spider.so というファイルが作成されますので、これを/usr/lib64/samba/vfs/に smb_spider.so という名称でコピーします。

※ 64bit 版の場合

- 5) smb と nmb のプロセスを再起動します。

5.7. ESS サーバとの接続

構築済みの ESS10 サーバに SSS を接続します。ESS サーバがインターネットに接続されていれば、SSS をインストールしたサーバがインターネットに接続していない状態でも、定義ファイルの更新が可能になります。

集中管理サーバの管理画面(ControlCenter)上の操作が必要ですので、アクセスできる状態で実施してください。

【注意】 Kernel バージョンが 2.6.37 より古い場合、SpIDer Guard の起動時に OS の再起動が発生する場合があります。その防止のため、集中管理サーバ上の設定を変更し、SpIDer Guard を無効化します。

下記のサービスにて、CentOS 6.x や CentOS 5.x を使用している場合は、必ず実行してください。

GMO クラウド社 : Altus Basic シリーズ、Altus Isolate シリーズ

※ SSS の設定にて SpIDer Guard の起動を停止している場合でも、ESS10 サーバに接続する際は必ず実施してください。

<無効化手順>

- i. 集中管理サーバにログインします。
- ii. 「アンチウィルスネットワーク」メニューを開きます。
- iii. 中央のツリーから、[Everyone]を選択します。
- iv. 「設定」セクションから[UNIX]-[Linux]-[SpIDer Guard]を開きます。
- v. 「全般」タブ内の「SpIDer Guard for Linux を有効にする」のチェックを外します。
- vi. 「保存」をクリックします。

- 1) ESS10 サーバより drwcsd.pub(公開鍵)ファイルをダウンロードします。

`http://<IP アドレス>:9080/install/drwcsd.pub`

※ ブラウザ等で以下にアクセスするとダウンロードできます。

※ drwcsd.pub ファイルは ESS サーバ毎に異なりますので、接続先サーバより入手してください。

- 2) 以下のコマンドを実行し、ESS10 サーバに接続します。

```
# drweb-ctl esconnect --key <path>drwcsd.pub <ESS10 サーバアドレス>:2193
```

例) ESS10 サーバのアドレスが 192.168.1.126、drwcsd.pub を/home/test に保存している場合

```
# drweb-ctl esconnect --key /home/test/drwcsd.pub 192.168.1.126:2193
```

※ 接続先サーバの IP アドレスやポートを誤って指定した場合は、以下のコマンドを実行後に再度実施してください。

```
# drweb-ctl esdisconnect
```



- 3) ESS10 サーバに接続されると以下のメッセージが表示されます。

```
Pending for approval from central protection server
#
```

※ 上記は、手動承認にしている場合の表示です。

- 4) ブラウザから ControlCenter にログインします。
- 5) 「アンチウィルスネットワーク」メニュー中央のツリーから、[Status]-[Newbies]を開きます。
- 6) 表示されている端末(SSS をインストールしたサーバ名が表示されます)を選択し、承認します。
- 7) 「アンチウィルスネットワーク」メニュー中央のツリーから、[Everyone]を開き、SSS をインストールしたサーバのアイコンが緑色の状態であることを確認します。
- 8) SSS をインストールしたサーバ上の `/var/opt/drweb.com/bases/drwtoday.vdb` が、更新されていることを確認します。

※ samba との連携設定が完了していない場合は、以下のスクリプトを実行し、その後 samba 関連プロセスの再起動を行なってください。

```
/opt/drweb.com/share/drweb-smbspider-modules/drweb_smbspider_configure.sh
```

※ ESS10 サーバと切断する場合(集中管理から外す場合)は、以下のコマンドを実行してください。

```
# drweb-ctl esdisconnect
```

5.8. OS が起動しない場合の対処

Kernel バージョンが 2.6.37 より古い環境(CentOS 5.x、CentOS 6.x、等)において、OS が起動しない(再起動を繰り返す)状態となった場合、以下の方法で SpIDer Guard を無効化してください。

- 1) シングルユーザモードで OS を起動します。

※ GMO クラウド社 Altus Basic シリーズ、Altus Isolate シリーズをご利用の方は、以下の URL の STEP1 を参考にレスキューモードで起動してください。

<https://support.gmocloud.com/pf/guide/basic/useful/plesk.html>

- 2) 以下の 2 つのサービスを起動しないよう変更します。

`drweb-configd`

`drweb-spider-kmod`

※ `rc*.d` フォルダ内の以下のファイルをリネームしてください。

変更前) `"S??drweb-configd"`、`"S??drweb-spider-kmod"`

変更後) `"K??drweb-configd"`、`"K??drweb-spider-kmod"`

- 3) OS を再起動します。

※ GMO クラウド社 Altus Basic シリーズ、Altus Isolate シリーズをご利用の方は、一度サーバを停止した後、1)で変更した内容を元に戻した状態で OS を起動してください。

- 4) `drweb` のプロセスが起動していないことを確認します。

```
# ps -ef | grep drweb
```

- 5) `drweb32.key` をリネームします。

```
# cd /etc/opt/drweb.com
```

```
# mv drweb32.key drweb32.key_org
```

- 6) `drweb-configd` を起動します。

```
# /etc/init.d/drweb-configd start
```

- 7) 以下のコマンドを実行し、SpIDer Guard の起動を停止します。

```
# drweb-ctl cfset LinuxSpider.Start No
```

- 8) 設定が変更されたことを確認します。

```
# drweb-ctl cfshow | grep "LinuxSpider.Start"
```

```
LinuxSpider.Start = No
```



- 9) drweb32.key を元の名前に戻します。

```
# cd /etc/opt/drweb.com  
# mv drweb32.key_org drweb32.key
```

- 10) drweb-configd を再起動します。

```
# /etc/init.d/drweb-configd restart
```

- 11) drweb-configd と drweb-spider-kmod サービスの起動設定を変更します。

```
# chkconfig drweb-configd on --level 235  
# chkconfig drweb-spider-kmod on --level 235
```

お使いの製品の詳細な機能の説明や、利用方法は、各製品マニュアルをご参照ください。また、製品のご利用について、ご質問やトラブル等がありましたら、ライセンス証書と併せてお送りしているサポート窓口まで、お気軽にお問い合わせください。

株式会社 Doctor Web Pacific

〒210-0005 神奈川県川崎市川崎区東田町 1-2NKF 川崎ビル 2F

TEL:044-201-7711 FAX:044-201-7712

URL: www.drweb.co.jp