



Dr.Web Server Security Suite Ver.11.0 簡易構築ガイド -Linux 用-

株式会社 Doctor Web Pacific

初版 : 2016/08/15

改訂 : 2019/02/05



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
1.3	システム要件.....	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
3.1.1	パッケージの確認.....	4
3.1.2	他のアンチウイルスのインストール状況の確認.....	4
3.2	リポジトリ設定.....	4
3.2.1	Cent OS 系.....	4
3.2.2	Ubuntu 系.....	4
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.	SSS のコンポーネントの更新.....	16
5.6.	定義ファイルの更新.....	17
5.7.	コマンドラインからのスキャンの実行等.....	18
5.8.	samba との連携.....	20
5.8.1	samba との連携時の設定.....	20
5.8.2	VFS SMB Module の作成.....	20
5.9.	ESS サーバとの接続.....	21
5.9.1	コマンドラインから実行する場合.....	21
5.9.2	Web インターフェースから実行する場合.....	22
5.10.	OS が起動しない場合の対処.....	25
5.11.	以前のバージョンの Dr.Web のアンインストール.....	26
5.11.1	Ver6 の場合.....	26
5.11.2	Ver10 の場合.....	28



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)

1.3 システム要件

システム要件につきましては、下記 URL をご参照ください。

https://download.geo.drweb.com/pub/drweb/unix/server/11.0/documentation/html/en/dw_9_sysrequirements.htm

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 7.2 (64bit)、Ubuntu 16.04 (64bit)
- samba のバージョン
 - Cent OS 7.2 : 4.2.10
 - Ubuntu 16.04 : 4.3.9
- selinux
 - 無効
- iptables(FireWall)
 - 無効



3. 準備

3.1 インストール環境の確認

3.1.1 パッケージの確認

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 7.2

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

➤ Ubuntu 16.04

libc6-i386、libc6、perl

3.1.2 他のアンチウイルスのインストール状況の確認

他のアンチウイルスがインストールされている場合、事前にアンインストールを実施してください。

また、Dr.Web の Ver10 以前がインストールされている場合は、「5.11 以前のバージョンの Dr.Web のアンインストール」に記載の手順に従い、事前にアンインストールを実施してください。

3.2 リポジトリ設定

SSS をリポジトリから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

以下のコマンドを実行してください。

```
# wget http://repo.drweb.com/drweb-repo11.rpm
# rpm -ivh drweb-repo11.rpm
```

3.2.2 Ubuntu 系

以下のコマンドを実行してください。

```
$ wget http://repo.drweb.com/drweb-repo11.deb
$ sudo dpkg -i drweb-repo11.deb
$ 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

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

➤ Ubuntu

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

- 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

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

➤ Ubuntu

```
$ 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、サービスを再起動します。

- CentOS

```
# 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

```
# drweb-ctl license  
License number <Key No.>, expires <ライセンス期限> (<残り日数>)
```

- Ubuntu

```
$ sudo drweb-ctl license  
License number <Key No.>, expires <ライセンス期限> (<残り日数>)
```

- 12) 以下のコマンドを実行し、SpIDer Guard for SMB (SMBSpider)と SpIDer Guard for Linux (LinuxSpider)を起動します。

※ **初期状態では、常駐保護機能は全て無効**となっております。

【注意】 Kernel バージョンが 2.6.37 より古い場合、SpIDer Guard for Linux (LinuxSpider)の起動時に OS の再起動が発生する場合がありますので、SpIDer Guard for Linux (LinuxSpider)は起動しないようにしてください。

下記サービスにて、CentOS 6.x や CentOS 5.x を使用している場合は、決して起動しないでください。

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

- CentOS

```
# drweb-ctl cfset SMBSpider.Start Yes  
# drweb-ctl cfset LinuxSpider.Start Yes
```

- Ubuntu

```
$ sudo drweb-ctl cfset SMBSpider.Start Yes  
$ sudo drweb-ctl cfset LinuxSpider.Start Yes
```




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、「yes」と入力し、「Enter」キーを押します。

```
Do you agree with the terms of this license? (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。

※ 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)
```

6) 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:
```

7) 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)
```



- 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。

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

- 9) 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:
```

- 10) 9)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)  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) 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)
```

- 12) 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。
ESS サーバと接続後に、SSS のコンポーネント(プログラム)の更新を実行してください。

- 13) 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。
14) 以下のコマンドを実行し、サービスを再起動します。

➤ CentOS

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

➤ Ubuntu

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

- 15) 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

```
# drweb-ctl license
```

```
License number <Key No.>, expires <ライセンス期限> (<残り日数>)
```

➤ Ubuntu

```
$ sudo drweb-ctl license
```

```
License number <Key No.>, expires <ライセンス期限> (<残り日数>)
```

- 16) 以下のコマンドを実行し、SSS のコンポーネント(プログラム)を更新します。

➤ CentOS

```
# yum update drweb*
```

➤ Ubuntu

```
$ sudo /opt/drweb.com/bin/zypper refresh
```

```
$ sudo /opt/drweb.com/bin/zypper update
```



17) 以下のコマンドを実行し、SpIDer Guard for SMB (SMBSpider)と SpIDer Guard for Linux (LinuxSpider)を起動します。

※ **初期状態では、常駐保護機能は全て無効**となっております。

【注意】 Kernel バージョンが 2.6.37 より古い場合、SpIDer Guard for Linux (LinuxSpider)の起動時に OS の再起動が発生する場合がありますので、SpIDer Guard for Linux (LinuxSpider)は起動しないようにしてください。

下記サービスにて、CentOS 6.x や CentOS 5.x を使用している場合は、決して起動しないでください。

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

➤ CentOS

```
# drweb-ctl cfset SMBSpider.Start Yes
# drweb-ctl cfset LinuxSpider.Start Yes
```

➤ Ubuntu

```
$ sudo drweb-ctl cfset SMBSpider.Start Yes
$ sudo drweb-ctl cfset LinuxSpider.Start Yes
```

18) 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 7.2 の場合を記載しております。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。

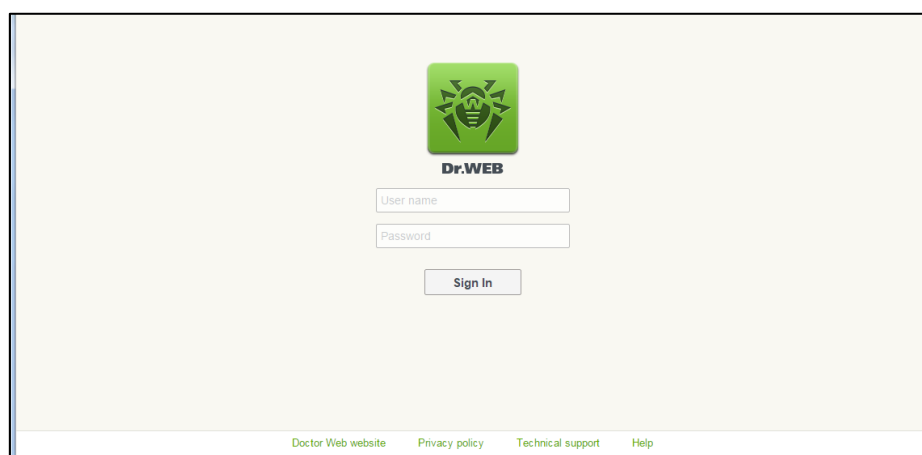
初期状態では、SSSをインストールしたサーバ上で以下のURLにアクセスすることにより、Web インターフェースを開くことができます。

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.WebConsoleAddress <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。

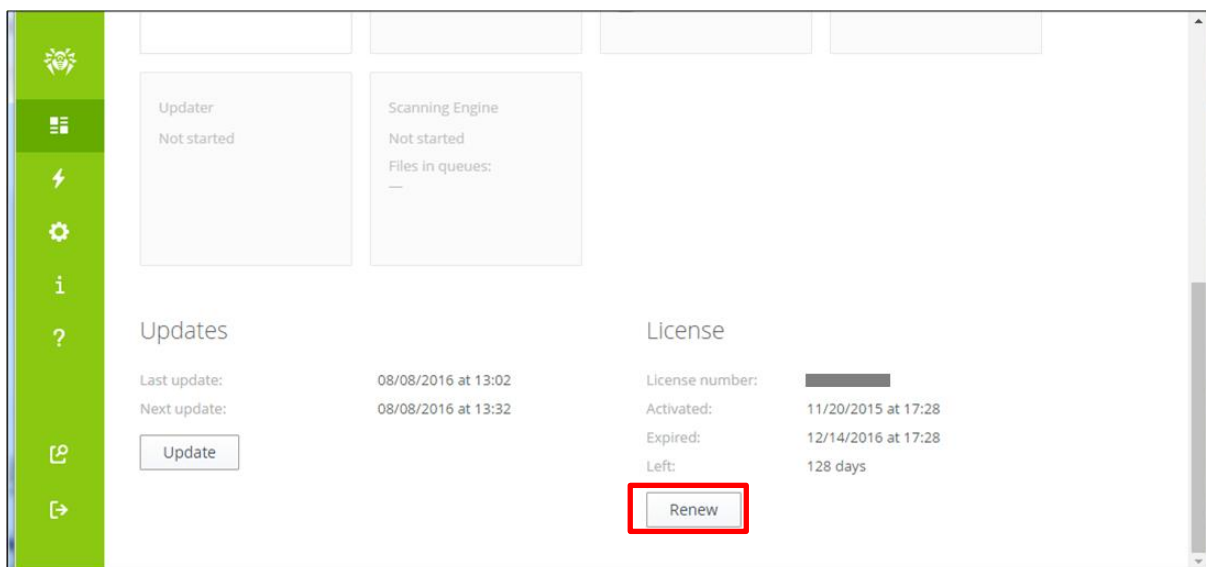
```
# /etc/init.d/drweb-configd restart
```

- 3) 以下のコマンドを実行して、新しいライセンスに更新されたことを確認します。

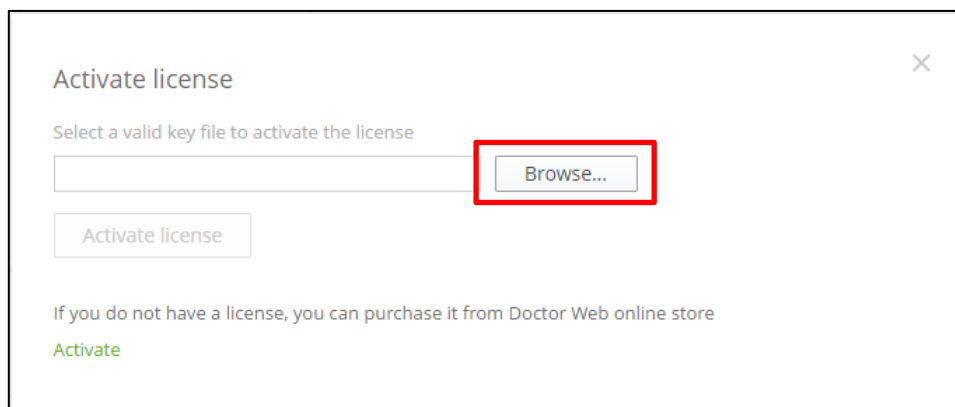
```
# drweb-ctl license  
License number <Key No.>, expires <ライセンス期限> (<残り日数>)
```

5.4.2 Web インターフェースからの更新

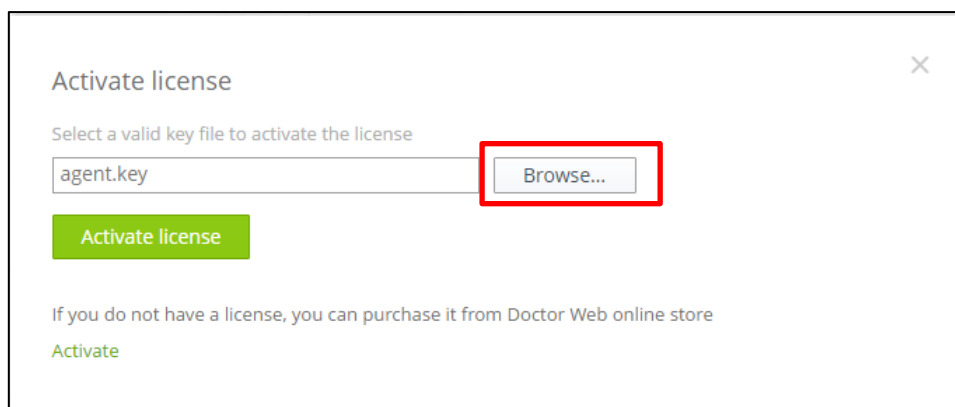
- 1) Web インターフェースにログインします。
- 2) [Main]メニュー内の License セクションの「Upload」ボタンをクリックします。



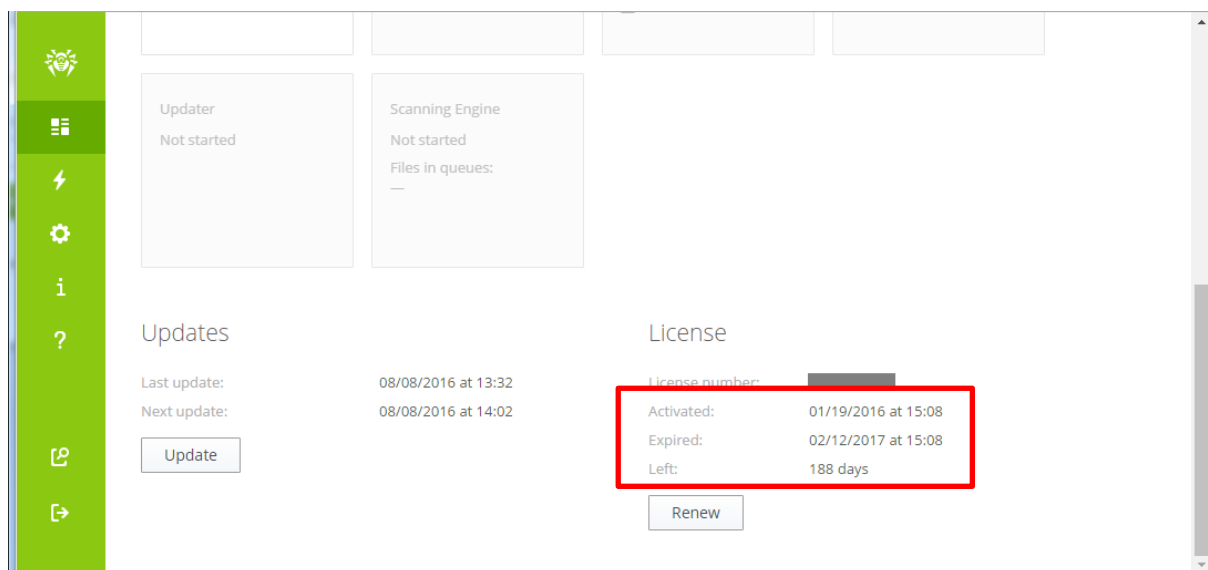
- 3) 「Browse」ボタンをクリックし、新しいライセンスキー(drweb32.key もしくは agent.key)を指定します。



- 4) 「Activate license」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) 以下のコマンドを実行して、新しいライセンスに更新されたことを確認します。

```
# drweb-ctl license
```

```
License number <Key No.>, expires <ライセンス期限> (<残り日数>)
```

5.5. SSS のコンポーネントの更新

SSS のコンポーネント(プログラム)は自動では更新されませんが、以下のコマンドを実行すると更新が可能です。

- 1) CentOS

```
# yum update drweb*
```

※ リポジトリからインストールした場合もインストーラ(.run)からインストールした場合も同じです。

- 2) Ubuntu

SSS のインストール方法によって、コマンドが異なりますのでご注意ください。

- インストーラ(.run)からインストールした場合

```
$ sudo /opt/drweb.com/bin/zypper refresh
```

```
$ sudo /opt/drweb.com/bin/zypper update
```

- リポジトリからインストールした場合

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

```
$ sudo apt-get dist-upgrade
```


5.6. 定義ファイルの更新

定義ファイルは、初期設定では 30 分間隔で自動更新されます。手動で更新する場合や更新間隔を変更する場合は、以下の手順にて実施できます。

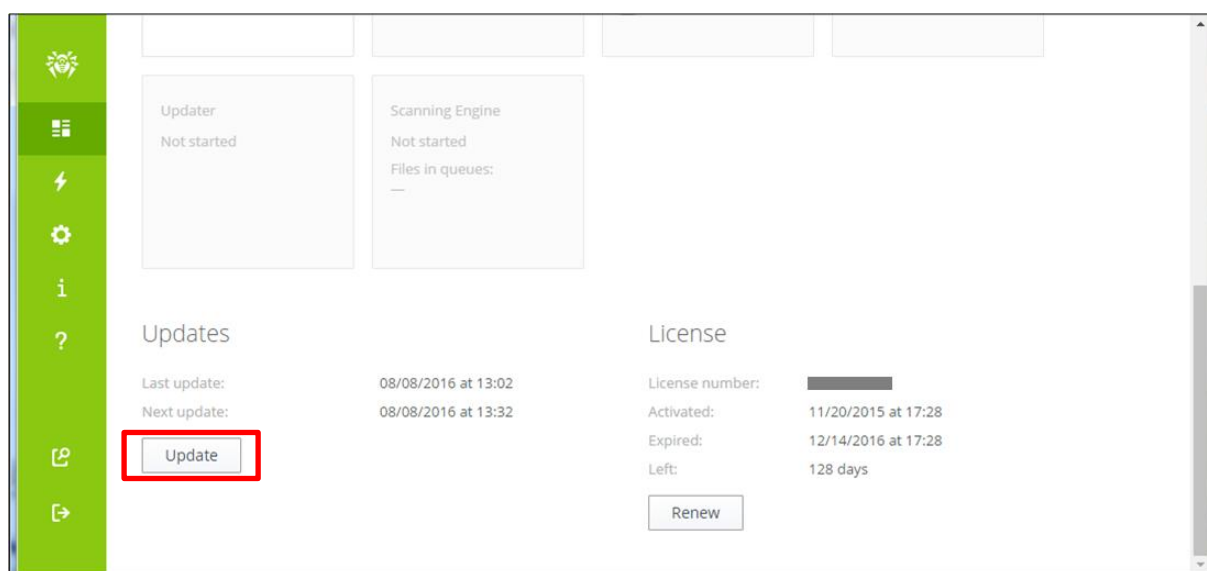
1) 手動更新

- コマンドラインから実行する場合

```
# drweb-ctl update
```

- Web インターフェースから実行する場合

[Main]メニュー内の Updates セクションの「Update」ボタンをクリックします。



2) 更新間隔の変更

- コマンドラインから実行する場合

下記は更新間隔を”60分”に変更する場合の例です。

```
# drweb-ctl cfset Update.UpdateInterval 60m
```

- Web インターフェースから実行する場合

[Settings]メニューから「Updater」を開き、「UpdateInterval」の値を変更します。更新間隔を”60分”に変更する場合は、「60m」と指定してください。

5.7. 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/11.0/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を行いません。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。

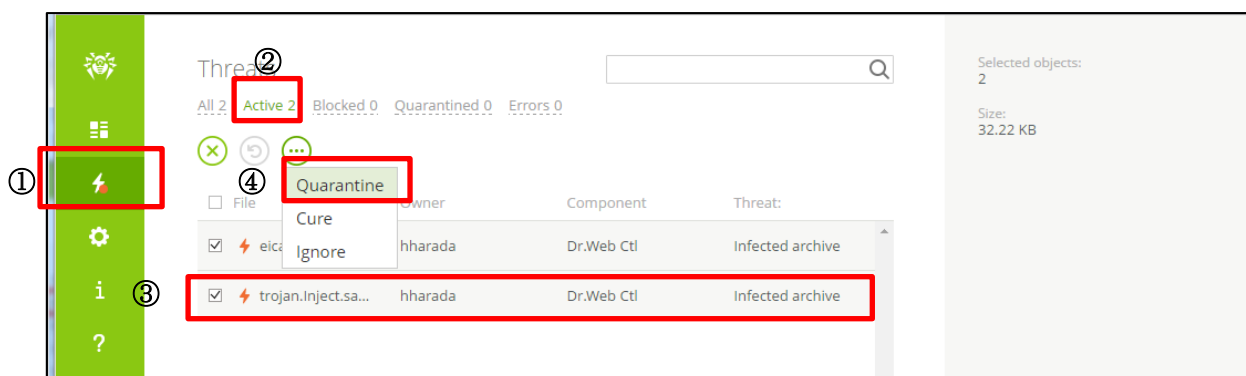
➤ コマンドラインから実行する場合

```
# 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、「More Actions」ボタンをクリックし表示された「Quarantine」すると、隔離処理が行われます。



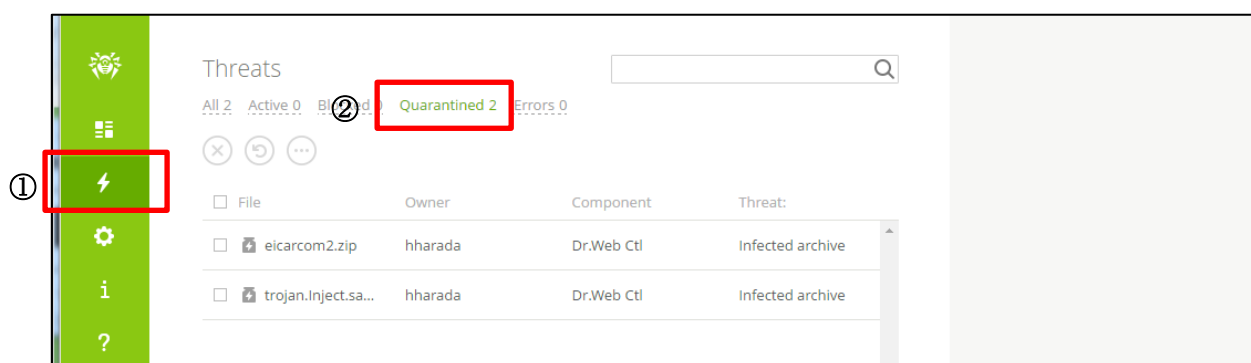
3) 隔離されたファイルの確認

- 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「Quarantined」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。





5.8. 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。

5.8.1 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、1 日後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。

項目名	初期値 ※コマンドラインでの表示	初期値 ※Web インターフェイスでの表示
AlertFiles ※警告ファイルの作成	Yes	“✓” ※有効
ActionDelay ※指定処理を行なうまでの待機時間	1d	1d
OnKnownVirus	Cure	Cure
OnIncurable	Quarantine	Quarantine
OnSuspicious	Quarantine	Quarantine
OnAdware	Pass	Skip
OnDialers	Pass	Skip
OnJokes	Pass	Skip
OnRiskware	Pass	Skip
OnHacktools	Pass	Skip

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

5.8.2 VFS SMB Module の作成

samba のいくつかのバージョンに対しては、VFS SMB Module が予め用意されています。しかしながら、ご利用される samba のバージョンによっては、VFS SMB Module を作成する必要があります。

詳しくは、「Dr.Web for UNIX File Servers」のマニュアルの[Components of the Product]-[SpIDer Guard for SMB]-[Building the VFS SMB Module]をご確認ください。



5.9. 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. 「アンチウイルスネットワーク」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。

5.9.1 コマンドラインから実行する場合

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`

※ 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
```

- ESS10 サーバに接続されると「Pending ...」のメッセージが表示され、承認されると「Accepted by ...」のメッセージが表示されます。

```
Pending for approval from central protection server
Accepted by tcp:// <ESS10 サーバアドレス>:2193
```

- ブラウザから ControlCenter にログインします。
- 「アンチウイルスネットワーク」メニュー中央のツリーから、[Status]-[Newbies]を開きます。
- 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。
- 「アンチウイルスネットワーク」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。
- 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
```

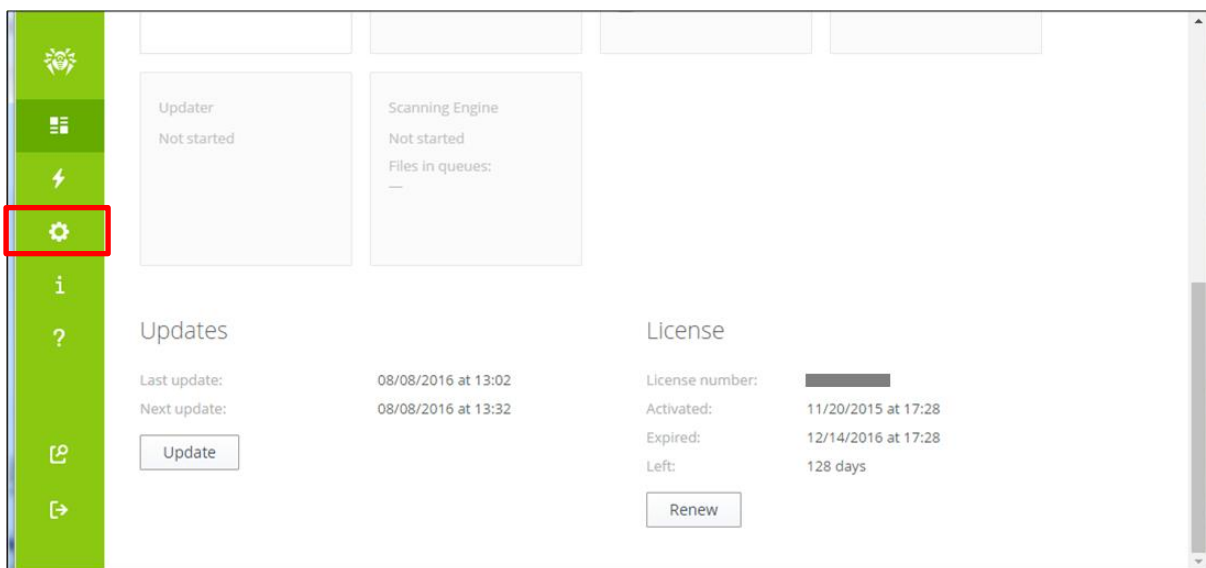
5.9.2 Web インターフェースから実行する場合

- 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。

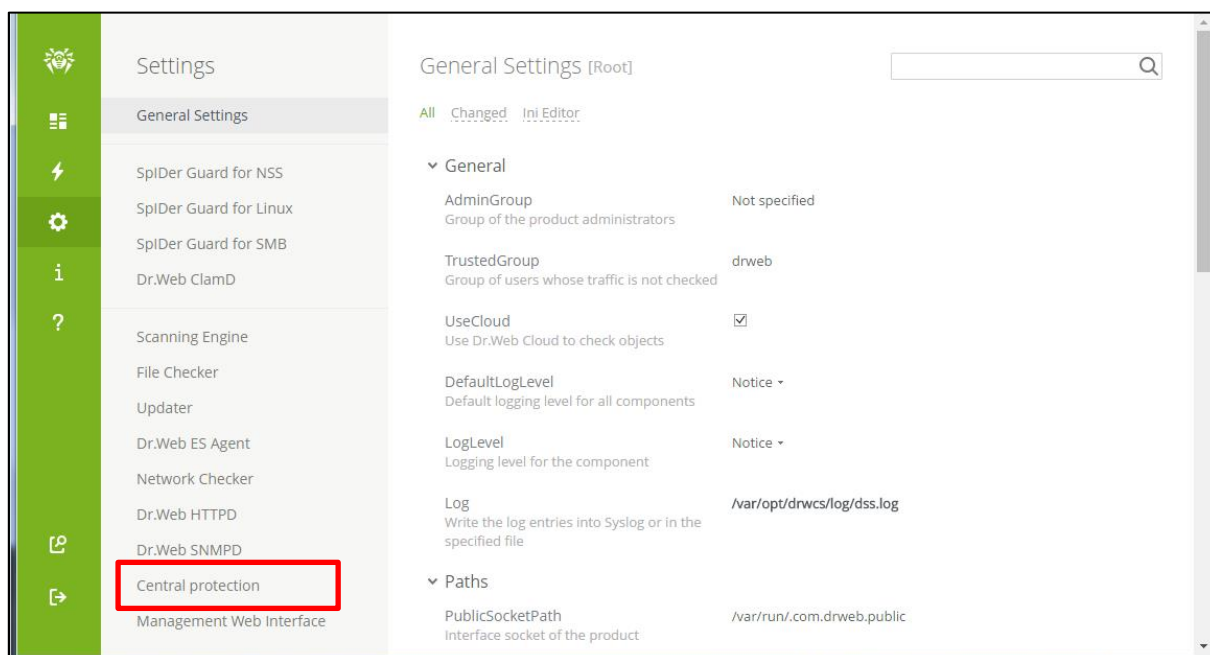
<http://<IP アドレス>:9080/install/drwcsd.pub>

※ 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。

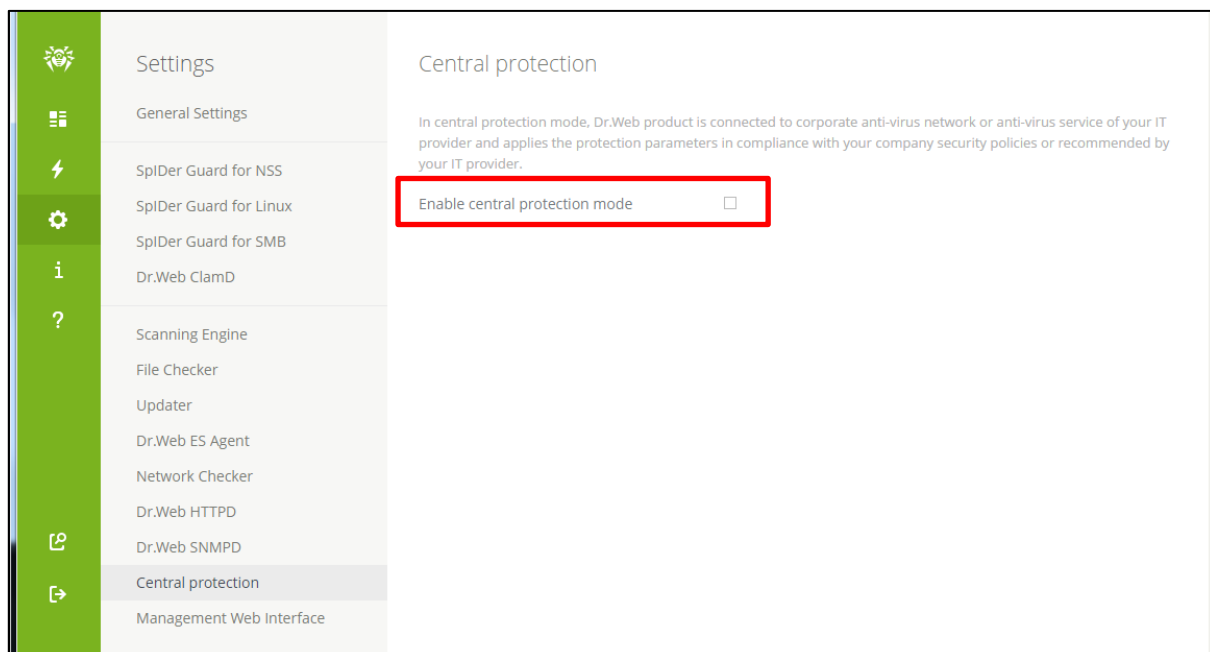
- Web インターフェースにログインします。
- [Settings]をクリックします。



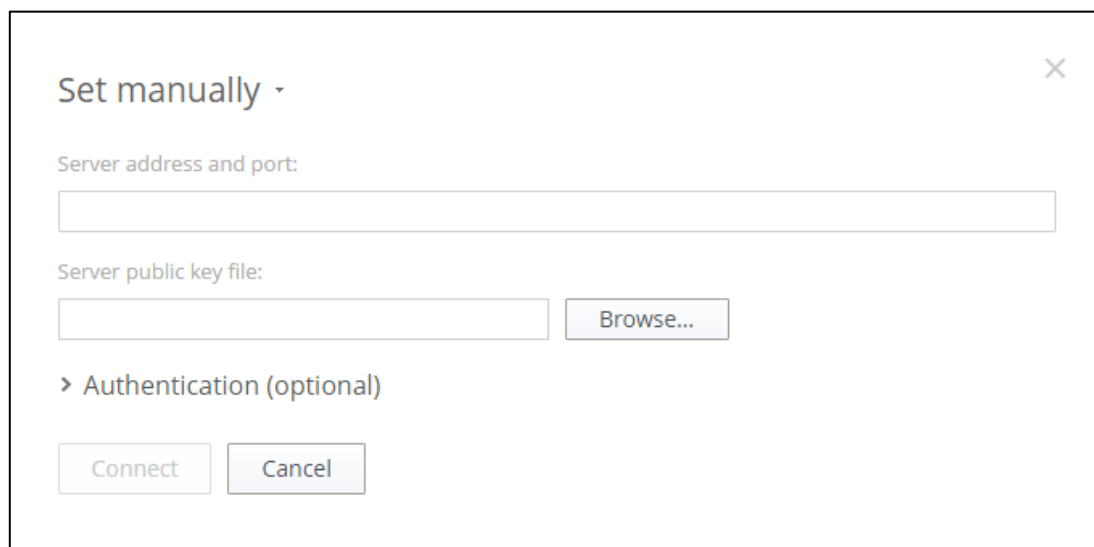
4) [Central protection]をクリックします。



5) “Enable central protection mode”にチェックを入れます。



- 6) 接続先サーバとポート番号(IP アドレス:2193)を指定し、「Browse」ボタンをクリックして drwcsd.pub を指定した後、「Connect」ボタンをクリックします。



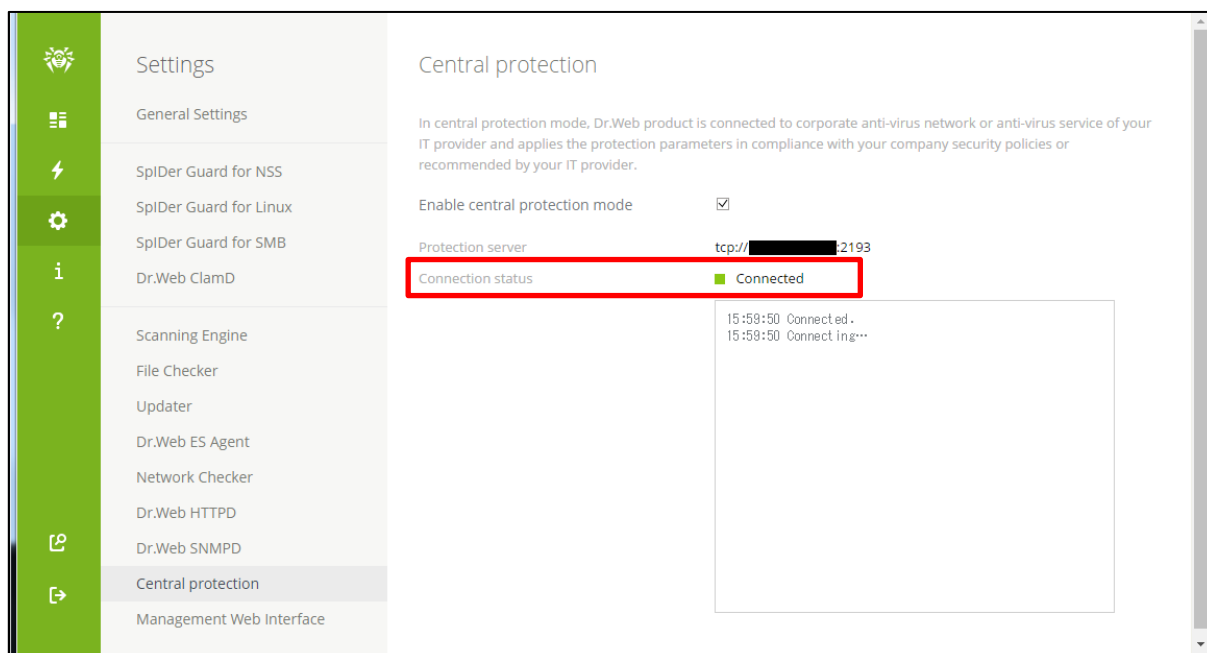
Set manually

Server address and port:

Server public key file:

> Authentication (optional)

- 7) ブラウザから ControlCenter にログインします。
- 8) 「アンチウイルスネットワーク」メニュー中央のツリーから、[Status]-[Newbies]を開きます。
- 9) 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。
- 10) Web インターフェース上で「Connection status」が「Connected」と表示されていることを確認します。



Settings

General Settings

SpiDer Guard for NSS

SpiDer Guard for Linux

SpiDer Guard for SMB

Dr.Web ClamD

Scanning Engine

File Checker

Updater

Dr.Web ES Agent

Network Checker

Dr.Web HTTPD

Dr.Web SNMPD

Central protection

Management Web Interface

Central protection

In central protection mode, Dr.Web product is connected to corporate anti-virus network or anti-virus service of your IT provider and applies the protection parameters in compliance with your company security policies or recommended by your IT provider.

Enable central protection mode

Protection server tcp://[redacted]:2193

Connection status Connected

15:59:50 Connected.
15:59:50 Connect ing...

※ ESS10 サーバと切断する場合(集中管理から外す場合)は、“Enable central protection mode”のチェックを外してください。



5.10. 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
```

5.11. 以前のバージョンの Dr.Web のアンインストール

以前のバージョンの Dr.Web がインストールされている場合は、以下の手順にてアンインストールしてください。
バージョンが不明な場合は、以下のコマンドを実行してご確認ください。

```
# /opt/drweb/drwebd -v
```

または、

```
# drweb-ctl -v
```

5.11.1 Ver6 の場合

- 1) samba のプロセス(smb および nmb)を停止します。
- 2) 以下のコマンドを実行します。

```
# /opt/drweb/remove.sh
```

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

```
This script will help you remove Dr.Web packages

Do you want to continue? (YES/no)
```



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

```
Select the software you want to remove:
  [] 1 Dr.Web Agent - Additional files to run Dr.Web Agent in central protection mode (6.0.2.4)
  [] 2 Dr.Web Agent (6.0.2.4)
~~ 略 ~~
  [] 17 Dr.Web Samba VFS Spider (6.0.2.4)
  [] 18 Dr.Web Updater (6.0.2.7)

To select a package you want to remove or deselect some previously
selected package - enter the corresponding package number and press Enter.

You may enter A or All to select all the packages, and N or None to deselect all of them.
Enter R or Remove to remove selected packages.
Enter 0, Q or Quit to quit the dialog.
All values are case insensitive.
Select:
```

- 5) 全ての項目が「X」となっていることを確認し、「R」と入力して、「Enter」キーを押します。

```
Select the software you want to remove:
  [X] 1 Dr.Web Agent - Additional files to run Dr.Web Agent in central protection mode (6.0.2.4)
  [X] 2 Dr.Web Agent (6.0.2.4)
~~ 略 ~~
  [X] 17 Dr.Web Samba VFS Spider (6.0.2.4)
  [X] 18 Dr.Web Updater (6.0.2.7)

To select a package you want to remove or deselect some previously
selected package - enter the corresponding package number and press Enter.

You may enter A or All to select all the packages, and N or None to deselect all of them.
Enter R or Remove to remove selected packages.
Enter 0, Q or Quit to quit the dialog.
All values are case insensitive.
Select:
```



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

```
A list of packages marked for removal:
  drweb-agent-es
  drweb-agent
  drweb-agent10-es
  ~~ 略 ~~
  drweb-scanner
  drweb-smbspider
  drweb-updater

Are you sure you want to remove the selected packages? (YES/no)
```

- 7) 以下のメッセージが表示されたことを確認します。

```
Removing empty installation directories...
Removal of drweb-updater is complete.
#
```

- 8) "/etc/samba/smb.conf"に追加されている、Dr.Web との連携用の以下の行をコメントアウトします。

```
vfs objects = smb_spider
```

※ 複数登録されている場合がありますので、全てコメントアウトしてください。

- 9) samba のプロセス(smb および nmb)の起動し、samba の共有フォルダにアクセスできることを確認します。

5.11.2 Ver10 の場合

- 1) samba のプロセス(smb および nmb)を停止します。
- 2) 以下のコマンドを実行します。

```
# /opt/drweb.com/bin/remove.sh
```

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

```
This script will help you remove Dr.Web packages

Do you wish to continue? (YES/no)
```



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

Select the software you want to remove:

1 Dr.Web Virus-Finding Engine and virus databases (10.1.0.1)

2 Boost, third party C++ libraries needed for Dr.Web product (10.1.0.0)

~~ 略 ~~

27 Dr.Web Updater - updating component for Dr.Web product (10.1.0.1)

28 Wt, third party C++ libraries needed for Dr.Web (10.1.0.1)

To select a package you want to remove or deselect some previously selected package - enter the corresponding package number and press Enter.

You may enter A or All to select all the packages, and N or None to deselect all of them.

Enter R or Remove to remove selected packages.

Enter 0, Q or Quit to quit the dialog.

All values are case insensitive.

Select:

- 5) 全ての項目が「X」となっていることを確認し、「R」と入力して、「Enter」キーを押します。

Select the software you want to remove:

1 Dr.Web Virus-Finding Engine and virus databases (10.1.0.1)

2 Boost, third party C++ libraries needed for Dr.Web product (10.1.0.0)

~~ 略 ~~

27 Dr.Web Updater - updating component for Dr.Web product (10.1.0.1)

28 Wt, third party C++ libraries needed for Dr.Web (10.1.0.1)

To select a package you want to remove or deselect some previously selected package - enter the corresponding package number and press Enter.

You may enter A or All to select all the packages, and N or None to deselect all of them.

Enter R or Remove to remove selected packages.

Enter 0, Q or Quit to quit the dialog.

All values are case insensitive.

Select:



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

```
A list of packages marked for removal:
  drweb-bases
  drweb-boost
  drweb-clamd
  ~ 略 ~
  drweb-spider
  drweb-update
  drweb-wt
Are you sure you want to remove the selected packages? (YES/no) Select:
```

- 7) 以下のメッセージが表示されたことを確認します。

```
Removing empty installation directories...
Running post-remove commands...
Removal of drweb-common is complete.
#
```

- 8) "/etc/samba/smb.conf"に追加されている、Dr.Web との連携用の以下の行をコメントアウトします。

vfs objects = smb_spider

※ 複数登録されている場合がありますので、全てコメントアウトしてください。

- 9) samba のプロセス(smb および nmb)の起動し、samba の共有フォルダにアクセスできることを確認します。



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、下記 URL よりお気軽にお問い合わせください。

https://support.drweb.co.jp/support_wizard/

株式会社 Doctor Web Pacific

〒105-0003 東京都港区西新橋 1-14-10 西新橋スタービル 2F

URL: www.drweb.co.jp