



Dr.Web Server Security Suite Ver.6.0.2.9 簡易構築ガイド -Linux 用-

株式会社 Doctor Web Pacific

初版 : 2015/10/27

改訂 : 2015/11/06



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. ESS サーバとの接続.....	13
5.1.1 ESS バージョン 10.....	13
5.1.2 ESS バージョン 6.....	14
5-2. ライセンス更新.....	15



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 5.10 (64bit)、Cent OS 6.5 (64bit)、Ubuntu Server 14.04 (64bit)
- 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 5.10

glibc.i686、glibc.x86_64、glibc-common.x86_64、perl

➤ Cent OS 6.5

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

➤ 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 – stable
baseurl=http://officeshield.drweb.com/drweb/el5/stable/x86_64/
gpgcheck=1
enabled=1
gpgkey=http://officeshield.drweb.com/drweb/drweb.key
```



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://officeshield.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://officeshield.drweb.com/drweb/debian stable 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 6 および 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
```

※ ESS サーバと接続させる場合は以降の手順は行わず、「5.1 ESS サーバとの接続」を参照してください。

- 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/opt/drweb/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 8)の手順は実行する必要はありません。

CentOS の場合

```
# /opt/drweb/scripts/drweb-smbspider/drweb_smbspider_configure.sh
```

Ubuntu の場合

```
# sudo /opt/drweb/scripts/drweb-smbspider/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) 以下のコマンドを実行し、drwebd サービスを起動します。

Cent OS 5.10、Cent OS 6.5 の場合

```
# /etc/init.d/drwebd start
```

Ubuntu の場合

```
# sudo /etc/init.d/drwebd start
```

- 10) 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。

Cent OS の場合

```
# cat /var/log/messages | grep "License key"
Oct 26 18:00:35 centos510 drwebd.real: License key number: <Key No. >
Oct 26 18:00:35 centos510 drwebd.real: License key activates: <有効化した日>
Oct 26 18:00:35 centos510 drwebd.real: License key expires: <ライセンス期限>
```

Ubuntu の場合

```
# sudo cat /var/log/syslog | grep "License key"
Oct 26 18:00:35 centos510 drwebd.real: License key number: <Key No. >
Oct 26 18:00:35 centos510 drwebd.real: License key activates: <有効化した日>
Oct 26 18:00:35 centos510 drwebd.real: License key expires: <ライセンス期限>
```

- 11) 以下のコマンドを実行し、drweb-monitor サービスを起動します。

Cent OS 5.10、Cent OS 6.5 の場合

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

Ubuntu の場合

```
# sudo /etc/init.d/drweb-monitor start
```

- 12) 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。



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 の場合

```
# ./<インストーラ名>
```

Ubuntu の場合

```
$ 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 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 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 the License Agreement? (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 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。

```
Updating RunAppList in /etc/drweb/monitor.conf .
/etc/drweb/monitor.conf is up-to-date, it is not necessary to modify it.
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、「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、「5.1 ESS サーバとの接続」を参照してください。

- 14) キーファイル(drweb32.key もしくは agent.key)を/opt/drweb/drweb32.key としてコピーします。
15) 以下のファイルを開き、「ENABLE=0」を「ENABLE=1」に変更します。

drwebd.enable、drweb-monitor.enable

- 16) 以下のコマンドを実行し、drwebd サービスを起動します。

Cent OS 5.10、Cent OS 6.5 の場合

```
# /etc/init.d/drwebd start
```

Ubuntu の場合

```
# sudo /etc/init.d/drwebd start
```



- 17) 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。

```
# cat /var/log/messages | grep "License key"  
Oct 26 18:00:35 centos510 drwebd.real: License key number: <Key No. >  
Oct 26 18:00:35 centos510 drwebd.real: License key activates: <有効化した日>  
Oct 26 18:00:35 centos510 drwebd.real: License key expires: <ライセンス期限>
```

※ Ubuntu の場合、sudo で実行してください。

- 18) 以下のコマンドを実行し、drweb-monitor サービスを起動します。

Cent OS 5.10、Cent OS 6.5 の場合

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

Ubuntu の場合

```
# sudo /etc/init.d/ drweb-monitor start
```

- 19) 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。



5. ケーススタディ

5-1. ESS サーバとの接続

構築済みの ESS 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。

5.1.1 ESS バージョン 10

- 1) ESS 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) ダウンロードした drwcsd.pub ファイルを/opt/drweb フォルダにコピーします。

- 3) /etc/drweb/agent.conf 内の[EnterpriseMode]セクションの下記を変更します。

- 集中管理モード(Enterprise モード)の使用

変更前 : `UseEnterpriseMode = no`

変更後 : `UseEnterpriseMode = yes`

- 接続先 ESS サーバの指定

変更前 : `ServerHost = 127.0.0.1`

変更後 : `ServerHost = <ESS サーバの IP アドレス>`

- 4) /etc/drweb/monitor.conf 内の[Monitor]セクションの下記を変更します。

変更前 : `UseEnterpriseMode = no`

変更後 : `UseEnterpriseMode = yes`

- 5) /etc/drweb/es_monitor.conf を変更し、以下の行のコメントアウトを解除します。

変更前 : `#Monitor/RunApplist DAEMON`

変更後 : `Monitor/RunApplist DAEMON`

- 6) `drwebd.enable` および `drweb-monitor.enable` を変更します。

変更前 : `ENABLE=0`

変更後 : `ENABLE=1`

- 7) /etc/drweb/drweb32.ini 内の[Scanner]セクションの下記を変更し、以下の行のコメントアウトを解除します。

変更前 : `# ControlAgent = local:/var/drweb/ipc/.agent`

変更後 : `ControlAgent = local:/var/drweb/ipc/.agent`

- 8) /etc/drweb/monitor/agent.mmc を変更します。

変更前 : `drweb-agent "-c /etc/drweb/agent.conf" 90 10 MAIL drweb:drweb`

変更後 : `drweb-agent10 "-c /etc/drweb/agent.conf" 90 10 MAIL drweb:drweb`



- 9) 以下のコマンドを実行し、drweb-monitor サービスを起動します。

Cent OS 5.10、Cent OS 6.5 の場合

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

Ubuntu の場合

```
# sudo /etc/init.d/drweb-monitor start
```

- 10) ブラウザから ControlCenter にログインします。
- 11) 「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。
- 12) 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。
- 13) 「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。
- 14) SSS をインストールしたサーバ上の/var/drweb/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/scripts/drweb-smbspider/drweb_smbspider_configure.sh
```

5.1.2 ESS バージョン 6

- 1) ESS 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) ダウンロードした drwcsd.pub ファイルを/opt/drweb フォルダにコピーします。
- 3) /etc/drweb/agent.conf 内の[EnterpriseMode]セクションの下記を変更します。
- 集中管理モード(Enterprise モード)の使用
変更前 : UseEnterpriseMode = no
変更後 : UseEnterpriseMode = **yes**
 - 接続先 ESS サーバの指定
変更前 : ServerHost = 127.0.0.1
変更後 : ServerHost = <ESS サーバの IP アドレス>
- 4) /etc/drweb/monitor.conf 内の[Monitor]セクションの下記を変更します。
- 変更前 : UseEnterpriseMode = no
変更後 : UseEnterpriseMode = **yes**



- 5) drwebd.enable および drweb-monitor.enable を変更します。

変更前 : ENABLE=0

変更後 : ENABLE=1

- 6) 以下のコマンドを実行し、drweb-monitor サービスを起動します。

Cent OS 5.10、Cent OS 6.5 の場合

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

Ubuntu の場合

```
# sudo /etc/init.d/drweb-monitor start
```

- 7) ブラウザから ControlCenter にログインします。
- 8) 「管理」メニューを開き、「未承認の端末」をクリックします。
- 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) 「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。
- 11) SSS をインストールしたサーバ上の/var/drweb/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/scripts/drweb-smbspider/drweb_smbspider_configure.sh
```

5-2. ライセンス更新

- 1) 新しいライセンスキー(drweb32.key もしくは agent.key)を/opt/drweb/drweb32.key としてコピーします。
- 2) drwebd および drweb-monitor のプロセスを再起動します。

Cent OS 5.10、Cent OS 6.5 の場合

```
# /etc/init.d/drwebd restart  
# /etc/init.d/drweb-monitor restart
```

Ubuntu の場合

```
# sudo /etc/init.d/drwebd restart  
# sudo /etc/init.d/drweb-monitor restart
```

- 3) /var/log/messages(Ubuntu の場合は、/var/log/syslog)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。



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