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

株式会社 Doctor Web Pacific

初版 ： 2018/08/28
改訂 ： 2019/02/06

目次

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、Gateway Security Suite(以下 GSS)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/gateway/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 6.10 (64bit)
- squid のバージョン

  squid : 3.1.23
- selinux

  無効
- FireWall(iptables, ip6tables)

  無効

3. 準備

3.1 インストール環境の確認

3.1.1 squid のビルドオプションの確認

以下のコマンドを実行して、インストールされている squid で"--enable-icap-client"オプションが有効化されているか確認してください。

```
# squid -v
```

※ "--enable-icap-client"オプションが有効化されていない場合、GSS を squid と連携させることはできません。

※ 出力される内容は、「6.6. squid のビルドオプションの確認例」を参照ください。

3.1.2 インストール済みパッケージの確認

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 6.10

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

3.1.3 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

インストールするバージョンよりも古い Dr.Web がインストールされている場合は、「6.9 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

GSS をリポジトリからインストールする場合、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
```

3.3 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、GSS 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 または 11)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。

  ※ インストーラは最新のものを使用してください。

  ※ 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、GSS のインストールを実行します。

```
# yum install drweb-internet-gateways
```

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) 以下のコマンドを実行し、サービスを再起動します。

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

4) 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。

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

5) 以下のコマンドを実行し、Dr.Web ICAPD を起動します。

```
# drweb-ctl cfset ICAPD.Start Yes
```

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。

```
# ./<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 Internet Gateways

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 the License Agreement? (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。

```
This installation script will help you to configure Dr.Web for UNIX Internet Gateways


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 key file or '0' to skip:
```

7) 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.
```

8) 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。

9) 以下のコマンドを実行し、サービスを再起動します。

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

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。

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

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

```
# yum update drweb*
```

12) 以下のコマンドを実行し、Dr.Web ICAPD を起動します。

```
# drweb-ctl cfset ICAPD.Start Yes
```

5. squid との連携設定と動作確認

5.1. 連携設定

GSS と squid を連携させるために、squid.conf を変更する必要があります。

1) squid.conf を変更します。

下記 URL の内容を参考に変更してください。インストールされている squid のバージョンにより設定内容が異なりますので注意してください。

https://download.geo.drweb.com/pub/drweb/unix/gateway/11.0/documentation/html/en/dw_9_squid_integration.htm

- squid バージョン 3.1

```
icap_enable on

icap_service i_req reqmod_precache bypass=0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache bypass=0 icap://127.0.0.1:1344/respmod

adaptation_access i_req allow all
adaptation_access i_res allow all

icap_preview_enable on
icap_preview_size 0

icap_send_client_ip on
icap_send_client_username on

icap_persistent_connections on
```

※ 上記は、squid がインストールされたサーバのアドレスが"127.0.0.1"(GSS と同一のサーバ)、ICAP 連携時に使用するポートが"1344"(GSS の初期値)の場合の例です。

- squid バージョン 3.2 以降

```
icap_enable on

icap_service i_req reqmod_precache bypass=0 icap://127.0.0.1:1344/reqmod
icap_service i_res respmod_precache bypass=0 icap://127.0.0.1:1344/respmod

adaptation_access i_req allow all
adaptation_access i_res allow all

icap_preview_enable on
icap_preview_size 0

adaptation_send_client_ip on
adaptation_send_username on

icap_persistent_connections on
```

※ 上記は、squid がインストールされたサーバのアドレスが”127.0.0.1”(GSS と同一のサーバ)、ICAP 連携時に使用するポートが”1344”(GSS の初期値)の場合の例です。

2) squid を再起動します。

```
# /etc/init.d/squid restart
# /etc/init.d/squid status
```

5.2. 動作確認

1) 以下のコマンドを実行して、GSS と squid の連携に使用される 1344 ポートがリッスンされているか確認します。

```
# netstat -an | grep 1344
tcp        0      0 127.0.0.1:1344          0.0.0.0:*               LISTEN
```

※ リッスンされていない場合、以下のコマンドを実行し、Dr.Web ICAPD を起動します。

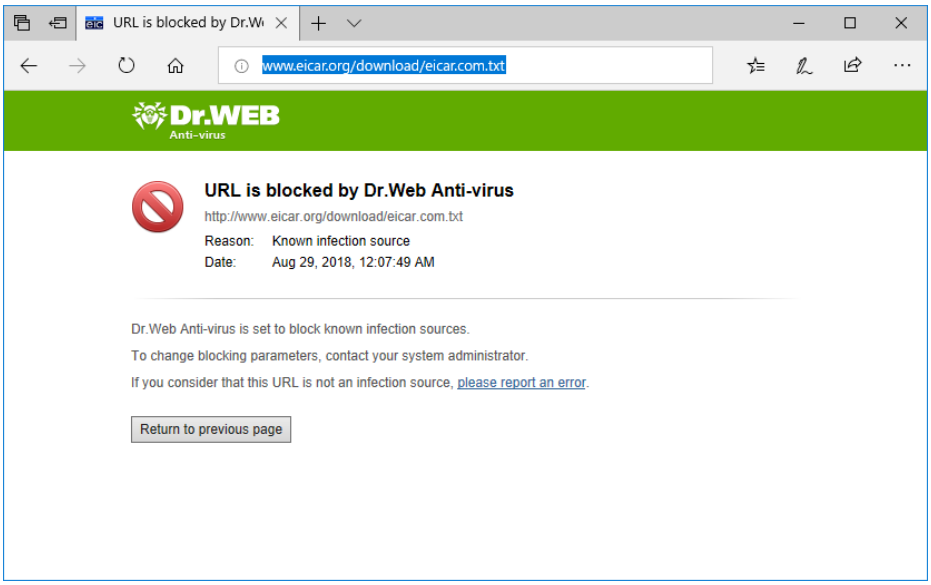
```
# drweb-ctl cfset ICAPD.Start Yes
```

2) 当該サーバをプロキシサーバとして使用した PC 上で、下記 URL にアクセスします。

http://www.eicar.org/download/eicar.com.txt

※ 上記 URL は、EICAR テストファイルのものとなります。

3) 以下のような画面がブラウザに表示されることを確認します。



※ /var/log/messages には、以下のような内容が出力されます。

```
Aug 29 00:22:13 staging64 drweb-icapd[45234]: Blocked URL: http://www.eicar.org/download/eicar.com.txt (Known infection source). User: Unknown from 192.168.1.104
```

6. ケーススタディ

6.1. 設定の確認と変更

6.1.1 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
```

6.1.2 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>
```

6.2. 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。

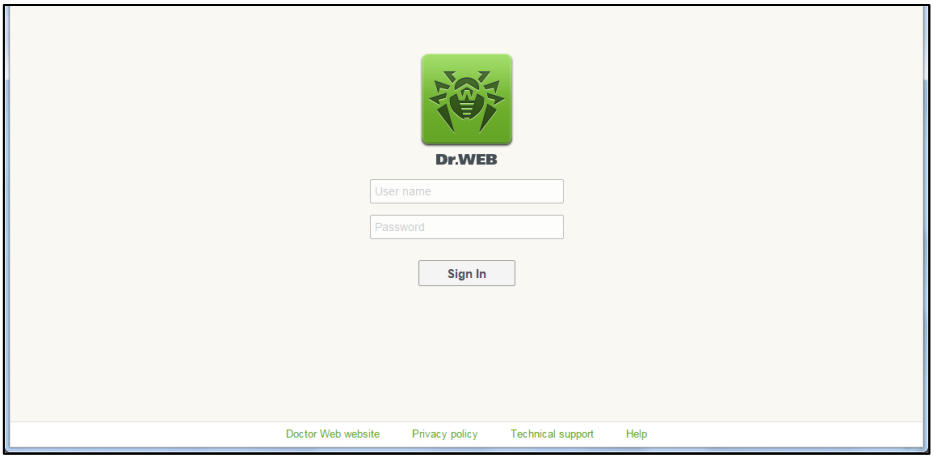
初期状態では、GSS をインストールしたサーバ上で以下の URL にアクセスすることにより、Web インターフェースを開くことができます。

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
```

6.3. ライセンス更新

6.3.1　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
```

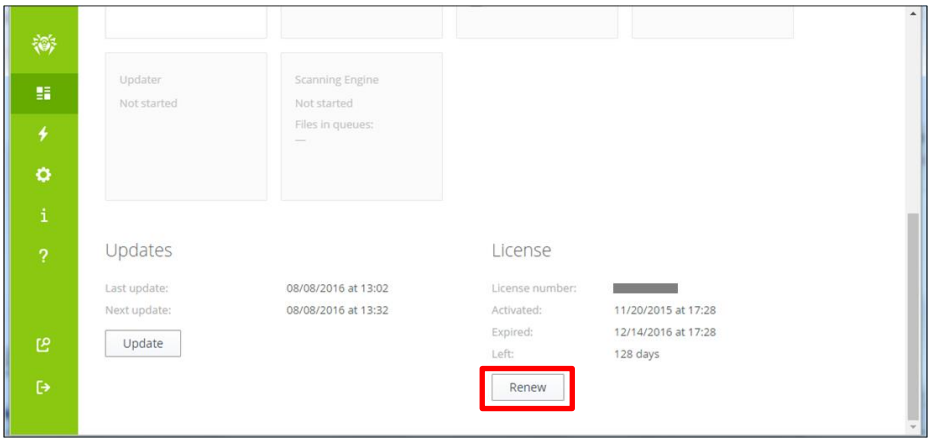
3) 以下のコマンドを実行して、新しいライセンスに更新されたことを確認します。

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

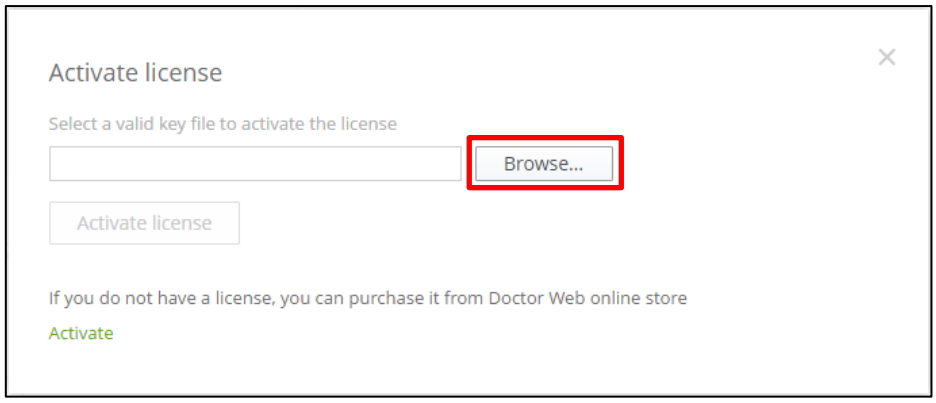
6.3.2　Web インターフェースからの更新

1) Web インターフェースにログインします。

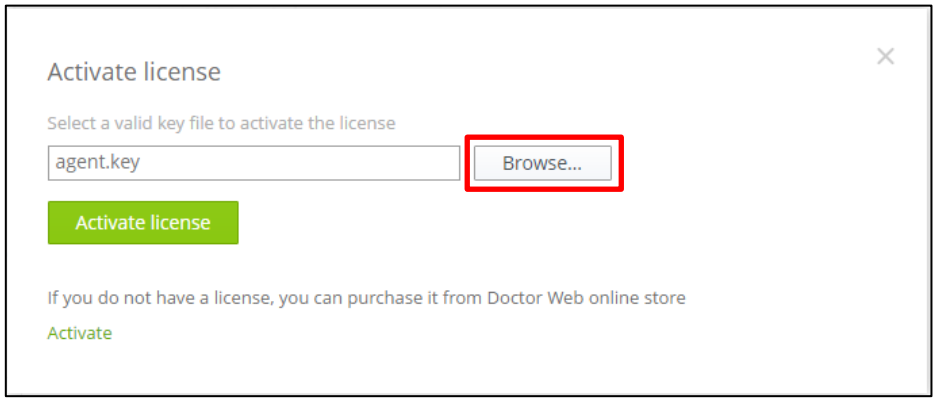
2) [Main]メニュー内の License セクションの「Upload」ボタンをクリックします。



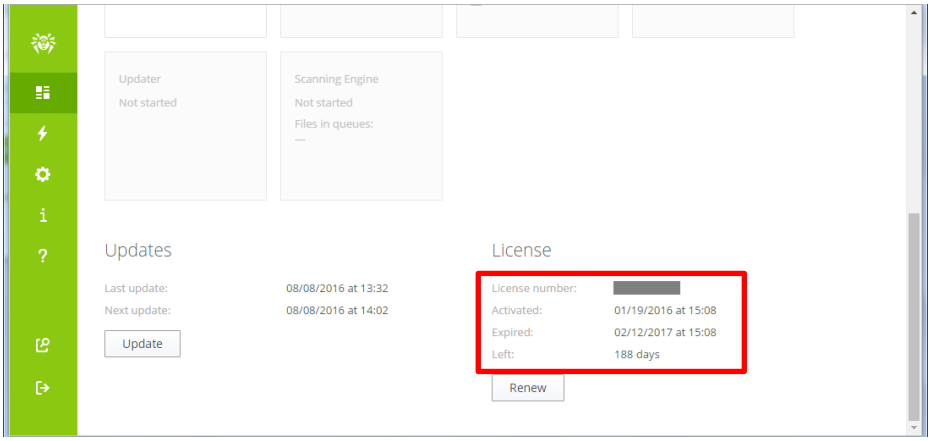
3) 「Browse」ボタンをクリックし、新しいライセンスキー(drweb32.key もしくは agent.key)を指定します。



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>)
```

6.4. 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。

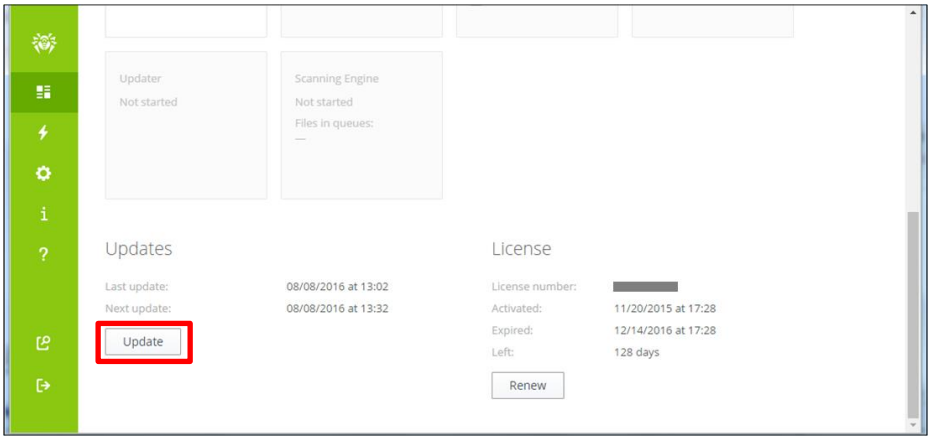
1) 手動更新

- 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。

6.5. GSS のコンポーネントの更新

GSS 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。

```
# yum update drweb*
```

6.6. squid のビルドオプションの確認例

6.6.1 GSS と連携可能な例

いずれも configure options に”--enable-icap-client”が表示されていますので、GSS と連携できます。

- Cent OS 6.10 の場合（squid を yum でインストール）

```
# squid -v
Squid Cache: Version 3.1.23
configure options:  '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--enable-internal-dns' '--disable-strict-error-checking' '--exec_prefix=/usr' '--libexecdir=/usr/lib64/squid' '--localstatedir=/var' '--datadir=/usr/share/squid' '--sysconfdir=/etc/squid' '--with-logdir=$(localstatedir)/log/squid' '--with-pidfile=$(localstatedir)/run/squid.pid' '--disable-dependency-tracking' '--enable-arp-acl' '--enable-follow-x-forwarded-for' '--enable-auth=basic,digest,ntlm,negotiate' '--enable-basic-auth-helpers=LDAP,MSNT,NCSA,PAM,SMB,YP,getpwnam,multi-domain-NTLM,SASL,DB,POP3,squid_radius_auth' '--enable-ntlm-auth-helpers=smb_lm,no_check,fakeauth' '--enable-digest-auth-helpers=password,ldap,eDirectory' '--enable-negotiate-auth-helpers=squid_kerb_auth' '--enable-external-acl-helpers=ip_user,ldap_group,session,unix_group,wbinfo_group' '--enable-cache-digests' '--enable-cachemgr-hostname=localhost' '--enable-delay-pools' '--enable-epoll' '--enable-icap-client' '--enable-ident-lookups' '--enable-linux-netfilter' '--enable-referer-log' '--enable-removal-policies=heap,lru' '--enable-snmp' '--enable-ssl' '--enable-storeio=aufs,diskd,ufs' '--enable-useragent-log' '--enable-wccpv2' '--enable-esi' '--enable-http-violations' '--with-aio' '--with-default-user=squid' '--with-filedescriptors=16384' '--with-dl' '--with-openssl' '--with-pthreads' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-linux-gnu' 'target_alias=x86_64-redhat-linux-gnu' 'CFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector --param=ssp-buffer-size=4 -m64 -mtune=generic -fpie' 'LDFLAGS=-pie' 'CXXFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector --param=ssp-buffer-size=4 -m64 -mtune=generic -fpie' --with-squid=/builddir/build/BUILD/squid-3.1.23
```

➢ Ubuntu 17.10 の場合（squid を apt-get でインストール）

```
$ sudo squid -v
Squid Cache: Version 3.5.23
Service Name: squid
Ubuntu linux
configure options:  '--build=x86_64-linux-gnu' '--prefix=/usr' '--includedir=${prefix}/include' '--mandir=
${prefix}/share/man' '--infodir=${prefix}/share/info' '--sysconfdir=/etc' '--localstatedir=/var' '--libexecdir=
${prefix}/lib/squid3' '--srcdir=.' '--disable-maintainer-mode' '--disable-dependency-tracking' '--disable-sil
ent-rules' 'BUILDCXXFLAGS=-g -O2 -fdebug-prefix-map=/build/squid3-0L3c88/squid3-3.5.23=. -fstack
-protector-strong -Wformat -Werror=format-security -Wno-error=deprecated -Wno-error=format-trunc
ation -Wdate-time -D_FORTIFY_SOURCE=2 -Wl,-Bsymbolic-functions -Wl,-z,relro -Wl,-z,now -Wl,--a
s-needed' '--datadir=/usr/share/squid' '--sysconfdir=/etc/squid' '--libexecdir=/usr/lib/squid' '--mandir=/us
r/share/man' '--enable-inline' '--disable-arch-native' '--enable-async-io=8' '--enable-storeio=ufs,aufs,disk
d,rock' '--enable-removal-policies=lru,heap' '--enable-delay-pools' '--enable-cache-digests' '--enable-icap-
client' '--enable-follow-x-forwarded-for' '--enable-auth-basic=DB,fake,getpwnam,LDAP,NCSA,NIS,PAM,
POP3,RADIUS,SASL,SMB' '--enable-auth-digest=file,LDAP' '--enable-auth-negotiate=kerberos,wrappe
r' '--enable-auth-ntlm=fake,smb_lm' '--enable-external-acl-helpers=file_userip,kerberos_ldap_group,LD
AP_group,session,SQL_session,time_quota,unix_group,wbinfo_group' '--enable-url-rewrite-helpers=fake
' '--enable-eui' '--enable-esi' '--enable-icmp' '--enable-zph-qos' '--enable-ecap' '--disable-translation' '--wi
th-swapdir=/var/spool/squid' '--with-logdir=/var/log/squid' '--with-pidfile=/var/run/squid.pid' '--with-filed
escriptors=65536' '--with-large-files' '--with-default-user=proxy' '--enable-build-info=Ubuntu linux' '--e
nable-linux-netfilter' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-g -O2 -fdebug-prefix-map=/build/squid
3-0L3c88/squid3-3.5.23=. -fstack-protector-strong -Wformat -Werror=format-security -Wall' 'LDFLAG
S=-Wl,-Bsymbolic-functions -Wl,-z,relro -Wl,-z,now -Wl,--as-needed' 'CPPFLAGS=-Wdate-time -D_FO
RTIFY_SOURCE=2' 'CXXFLAGS=-g -O2 -fdebug-prefix-map=/build/squid3-0L3c88/squid3-3.5.23=. -fs
tack-protector-strong -Wformat -Werror=format-security -Wno-error=deprecated -Wno-error=format-tr
uncation'
```

6.6.2 GSS と連携不可の例

configure options に"--enable-icap-client"がありませんので、GSS と連携できません。

- Cent OS 7.5 の場合（squid を yum でインストール）

```
# squid -v
Squid Cache: Version 3.5.20
Service Name: squid
configure options:  '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--disable-strict-error-checking' '--exec_prefix=/usr' '--libexecdir=/usr/lib64/squid' '--localstatedir=/var' '--datadir=/usr/share/squid' '--sysconfdir=/etc/squid' '--with-logdir=$(localstatedir)/log/squid' '--with-pidfile=$(localstatedir)/run/squid.pid' '--disable-dependency-tracking' '--enable-eui' '--enable-follow-x-forwarded-for' '--enable-auth' '--enable-auth-basic=DB,LDAP,MSNT-multi-domain,NCSA,NIS,PAM,POP3,RADIUS,SASL,SMB,SMB_LM,getpwnam' '--enable-auth-ntlm=smb_lm,fake' '--enable-auth-digest=file,LDAP,eDirectory' '--enable-auth-negotiate=kerberos' '--enable-external-acl-helpers=file_userip,LDAP_group,time_quota,session,unix_group,wbinfo_group,kerberos_ldap_group' '--enable-cache-digests' '--enable-cachemgr-hostname=localhost' '--enable-delay-pools' '--enable-epoll' '--enable-ident-lookups' '--enable-linux-netfilter' '--enable-removal-policies=heap,lru' '--enable-snmp' '--enable-ssl-crtd' '--enable-storeio=aufs,diskd,rock,ufs' '--enable-wccpv2' '--enable-esi' '--enable-ecap' '--with-aio' '--with-default-user=squid' '--with-dl' '--with-openssl' '--with-pthreads' '--disable-arch-native' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-linux-gnu' 'CFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches   -m64 -mtune=generic -fpie' 'LDFLAGS=-Wl,-z,relro  -pie -Wl,-z,relro -Wl,-z,now' 'CXXFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -grecord-gcc-switches   -m64 -mtune=generic -fpie' 'PKG_CONFIG_PATH=:/usr/lib64/pkgconfig:/usr/share/pkgconfig'
```

6.7. 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は行いません。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。

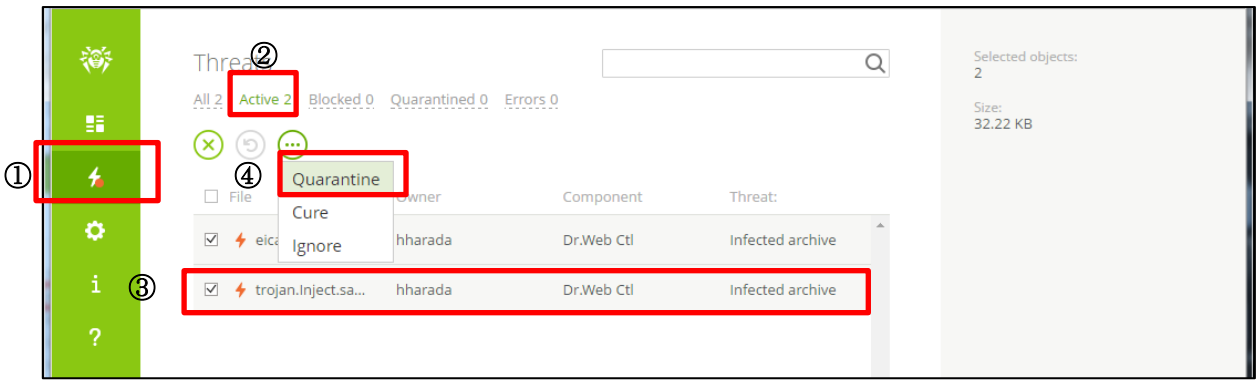
- コマンドラインから実行する場合

```
# 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。

6.8. ESS サーバとの接続

構築済みの ESS(バージョン 10 またはバージョン 11)サーバに GSS 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、GSS 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。

6.8.1 コマンドラインから実行する場合

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

※ 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、ESS 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) ESS 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
```

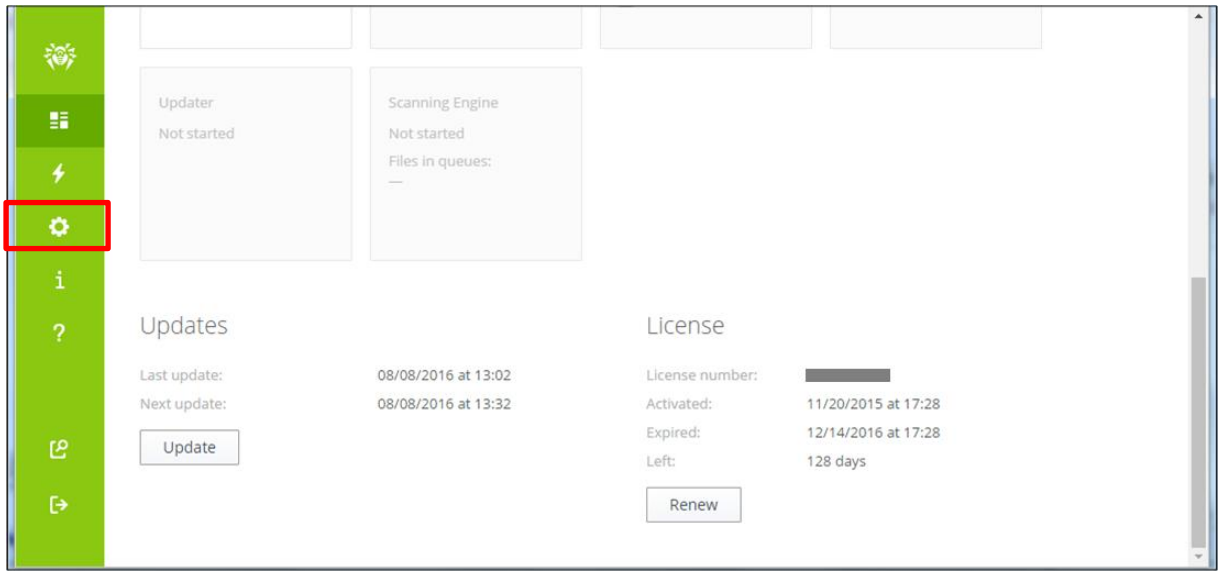
3) ESS サーバに接続されると「Pending ・・・」のメッセージが表示され、承認されると「Accepted by ・・・」のメッセージが表示されます。

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

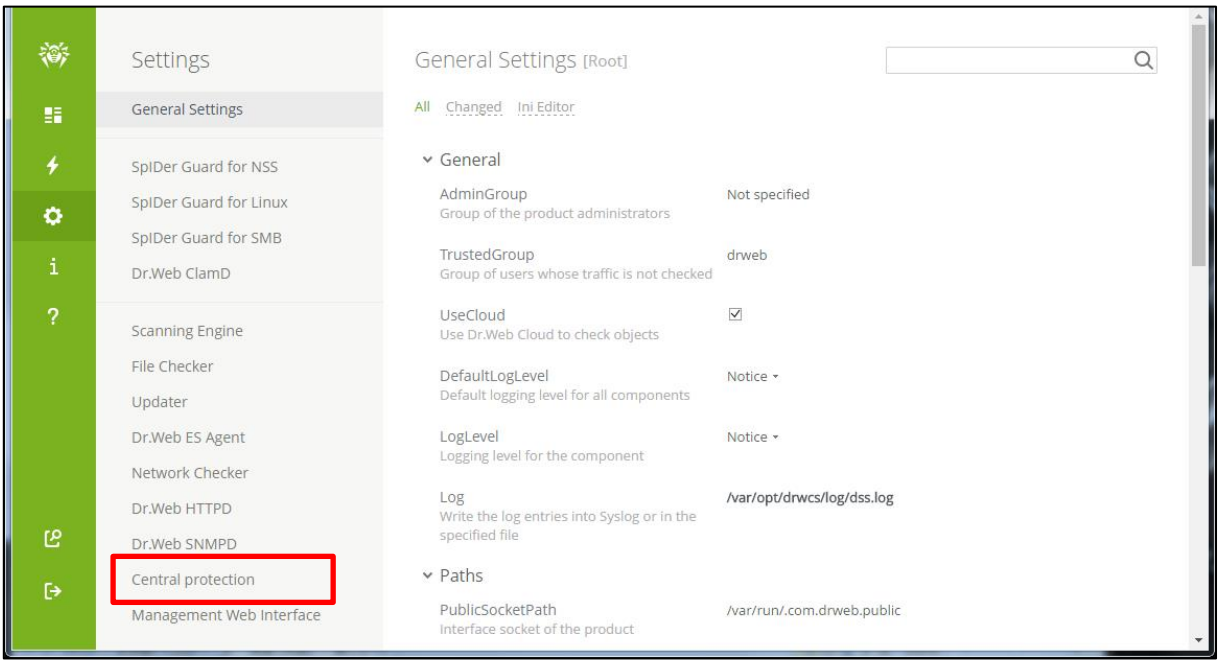
4) ブラウザから ControlCenter にログインします。
5) 「アンチウィルスネットワーク」メニュー中央のツリーから、[Status]-[Newbies]を開きます。
6) 表示されている端末(GSS をインストールしたサーバ名が表示されます)を選択し、承認します。
7) 「アンチウィルスネットワーク」メニュー中央のツリーから、[Everyone]を開き、GSS をインストールしたサーバのアイコンが緑色の状態であることを確認します。
8) GSS をインストールしたサーバ上の/var/opt/drweb.com/bases/drwtoday.vdb が、更新されていることを確認しま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

6.8.2 Web インターフェースから実行する場合

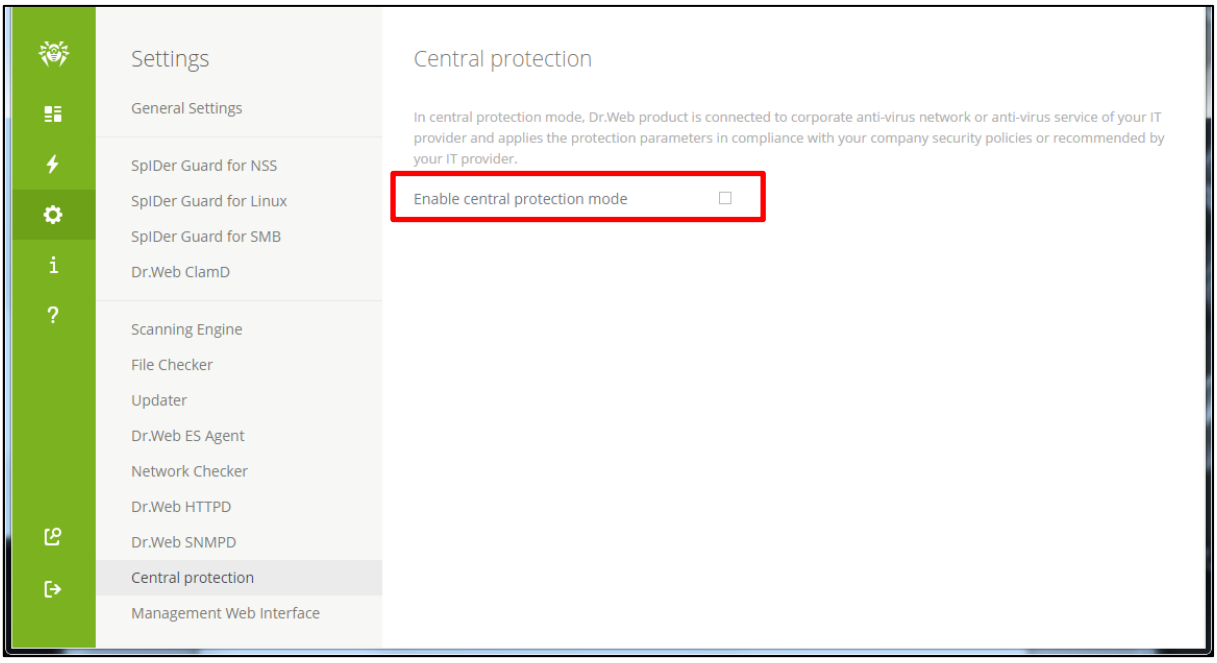
1) ESS サーバより drwcsd.pub(公開鍵)ファイルをダウンロードします。
http://<IP アドレス>:9080/install/drwcsd.pub
※ drwcsd.pub ファイルは ESS サーバ毎に異なりますので、接続先サーバより入手してください。
2) Web インターフェースにログインします。
3) [Settings]をクリックします。



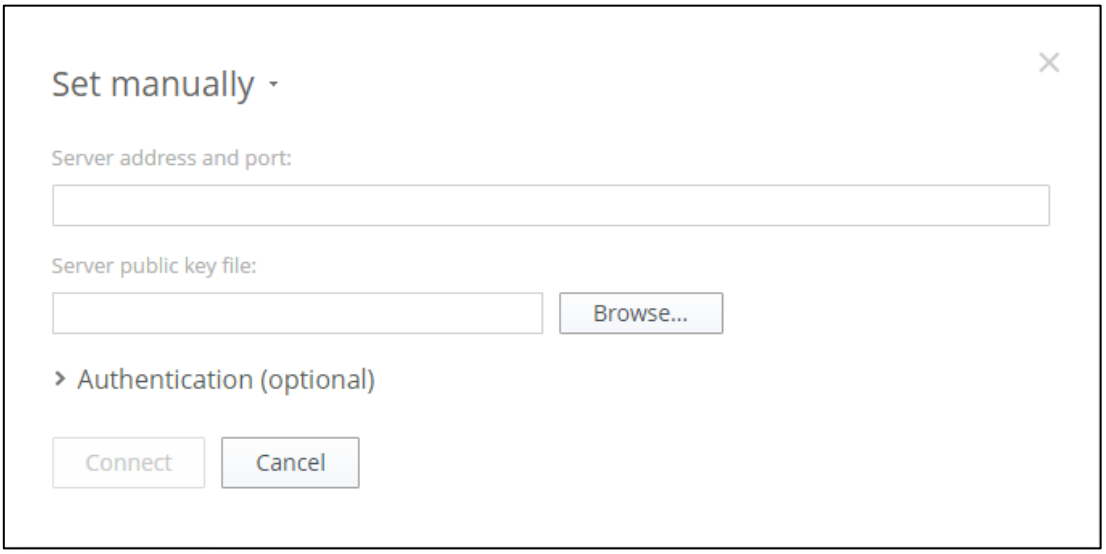
4) [Central protection]をクリックします。



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。

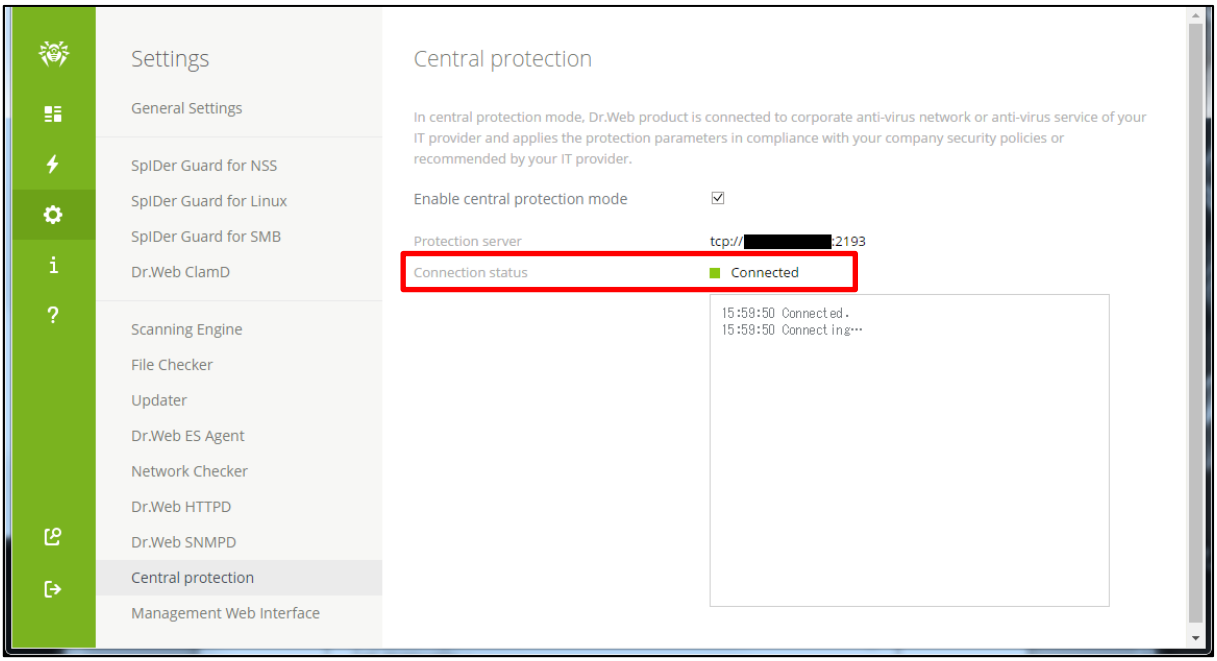


7) ブラウザから ControlCenter にログインします。

8) 「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。

9) 表示されている端末(GSS 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。



※ ESS 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。

6.9. 以前のバージョンの Dr.Web のアンインストール

1) squid のプロセスを停止します。

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 ~~
        [ ] 13 Dr.Web ICAP Daemon (6.0.2.4)
        [ ] 14 Dr.Web internet gateways documentation (6.0.2.9)
        [ ] 15 Essential third party libraries needed for Dr.Web on x86_64 systems (6.0.2.1)
        [ ] 16 Essential third party libraries needed for Dr.Web on x86 systems (6.0.2.1)
        [ ] 17 Dr.Web Monitor (6.0.2.3)
        [ ] 18 Dr.Web Antivirus Scanner (6.0.2.3)
        [ ] 19 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] 13 Dr.Web ICAP Daemon (6.0.2.4)
        [X] 14 Dr.Web internet gateways documentation (6.0.2.9)
        [X] 15 Essential third party libraries needed for Dr.Web on x86_64 systems (6.0.2.1)
        [X] 16 Essential third party libraries needed for Dr.Web on x86 systems (6.0.2.1)
        [X] 17 Dr.Web Monitor (6.0.2.3)
        [X] 18 Dr.Web Antivirus Scanner (6.0.2.3)
        [X] 19 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
~~ 略 ~~
        drweb-icapd
        drweb-internet-gateways-doc
        drweb-libs
        drweb-libs32
        drweb-monitor
        drweb-scanner
        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/squid/squid.conf"に追加されている、Dr.Web との連携用の行をコメントアウトします。

- squid バージョン 3.1 の場合の例

```
icap_service service_1 respmod_precache bypass=0
icap://localhost:1344/respmod
adaptation_access service_1 allow all
icap_preview_enable on
icap_preview_size 0
icap_send_client_ip on
icap_persistent_connections on
```

9) squid のプロセスを起動し、squid 経由で yahoo!等の URL 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