Dr.Web Enterprise Security Suite Ver.12
バージョンアップ(10→12)ガイド
-Linux 用-

株式会社 Doctor Web Pacific

初版 ： 2019/11/15
改訂 ： 2020/07/16

目次

1. はじめに

本書は、Dr.Web Enterprise Security Suite バージョン 10.01 (以降、ESS10)からバージョン 12(以下、ESS12)にアップグレードする為の手順をまとめています。ファイルやフォルダの PATH は、初期値の状態で記載しております。

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。また、構築の手順については、簡易構築ガイドを参照ください。

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。

- Cent OS 7.0 (64bit)
- Firewalld、SELinux は無効
- ESS12 がサポートする Linux 上に ESS バージョン 10.01 がインストールされていること。
- Windows 用 Agent については、最新の状態にコンポーネントが更新されていること。
- データベースは、SQLite3 を使用していること。
  ※ IntDB を使用している場合、SQLite3 に変更後に ESS11 へアップグレードしてください。
- ESS10 がインストールされた端末に、ESS12 をインストールし、環境を引き継ぐこと。
- 管理対象端末の OS が以下のリストに記載されていること。
  https://download.geo.drweb.com/pub/drweb/esuite/12.0.0/documentation/html/ja/appendices/app_sysreq.htm
  ※ Mac OS や Unix 向けの弊社製品を管理対象にされる場合、バージョンアップが必要となることがあります。
- 最新の ESS12 のインストーラを使用すること。

3. バージョンアップ作業の流れ

1) ESS10 のバックアップの取得
2) ESS10 のアンインストールと ESS12 のインストール
3) Windows 用 Agent の更新
4) Dr.Web Server 等設定変更

4. バージョンアップ

4.1 ESS10 のバックアップの取得

以下の ESS10 の設定ファイルやデータベース等のバックアップを取得してください。

※ 可能であれば、"/var/opt/drwcs/"をフォルダごとバックアップしてください。

- サーバスケジュール

  Control Center の「Dr.Web Enterprise サーバ schedule」から、設定済みサーバスケジュールをエクスポートしてください。

- キーファイル

  Control Center の「ライセンスマネージャー」から、Agent.key をエクスポートしてください。

- 設定ファイル等

  "/var/opt/drwcs/etc"フォルダを丸ごとバックアップしてください。

- 暗号化キー等

  Control Center の「暗号化キー」から、パブリックキーとプライベートキーをエクスポートしてください。また、"/opt/drwcs/Installer/"フォルダを丸ごとバックアップしてください。

- SQLite3

  ESS10 を停止し、以下のファイルをバックアップしてください。また、バックアップ取得後は、ESS10 を起動しないでください。

  /var/opt/drwcs/database.sqlite

※ IntDB を使用している場合、SQLite3 に変更後に ESS12 へアップグレードしてください。

また、必要に応じて重要なファイルのバックアップも取得してください。

※ CC の設定ファイルやレポートのテンプレート等

4.2 ESS10 のアンインストールと ESS12 のインストール

【注意】 DB として IntDB を使用している場合は、以降の手順を進める前に、SQLite3 への変更とデータ移行を実行してください。

1) Control Center に接続中の Agent が無いことを確認します。

※ ESS12 のインストールが完了するまで、Agent が ESS に接続しないようにしてください。

2) ESS10 を停止します。

```
# /etc/init.d/drwcsd stop
```

※ 停止後、drwcsd のプロセスが動作していないことを確認してください。

3) SQLite3 をファイルにエクスポートします。

```
# /etc/init.d/drwcsd exportdb /var/opt/drwcs/etc/esbase.es
```

4) エクスポートされたファイル(esbase.es)をホームディレクトリ等にコピーします。

5) ESS10 をアンインストールします。

```
# rpm -e drweb-esuite
```

6) ESS12 のインストーラに実行権を付与します。

```
# chmod +x <インストーラ名>
```

※ インストーラは、予めダウンロードしておいてください。OS 等によりインストーラ名は異なります。

7) インストーラを実行します。

```
# ./<インストーラ名>
```

※ ファイルの解凍が始まります。

8) 「License Agreement」が表示されたら、内容をよく確認します。

※ 次のページの内容を参照する場合は、スペースキーを押してください。

9) 「To continue the installation, you must accept the License Agreement. Accept?」と確認が表示されるので、「yes」と入力し、Enter キーを押します。

※ 何も入力せずに Enter キーを押した場合は、インストールが終了します。

10) 以下の内容が表示されたら、そのまま Enter キーを押します。

```
To use settings from the previous installation, set the path to the backup.
To use the backup from the default path (/var/tmp/drwcs), press Enter.
To install the Server with default settings not using backup ones, enter 0.

:
```

※ ESS10 のアンインストール時に作成されたバックアップデータが使用されます。

※ ユーザ、グループの作成、ファイルのコピー等が開始します。

11) 以下のメッセージが表示され、ESS12 のインストールが完了したことを確認します。

```
Database already exists.
Upgrading existing database (if required) ...
DB imported from the backup.
Upgrading existing database (if required) ...
Making initial product revision ...
Installation of drweb-esuite is complete.

Installation completed.
#
```

12) 以下のコマンドを実行し、drwcsd のプロセスが開始していることを確認します。

```
# /etc/init.d/drwcsd status
Dr.Web Server is started
#
```

4.3 管理画面(Control Center)での確認

インストールが完了したら、実際に管理画面(Control Center)へログイン可否等を確認します。

1) ブラウザから以下の URL にアクセスします。

http://<ESS サーバの IP アドレス or DNS 名>:9080/

https://<ESS サーバの IP アドレス or DNS 名>:9081/

※ http でアクセスした場合でも、https にリダイレクトされます。

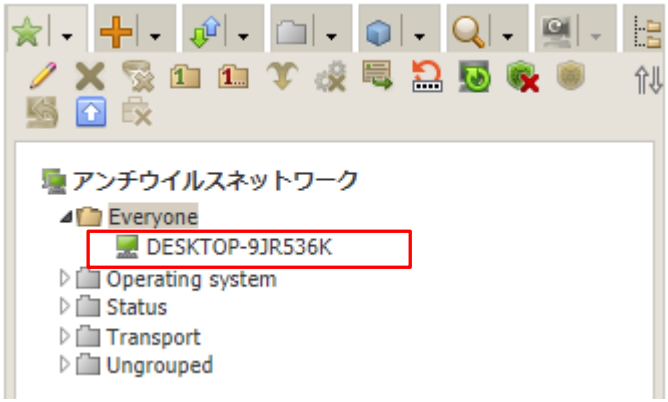
※ ブラウザによっては、「このサイトは安全ではありません」や「この接続ではプライバシーが保護されません」等のメッセージが表示されますので、「詳細」や「詳細設定」をクリックし、当該ページにアクセスしてください。

2) ID と Password を入力し、Control Center(以降、CC)にログインします。

ID : admin

Password : ESS10 と同じ

3) 画面中央の「アンチウイルスネットワーク」ツリーの「Everyone」グループ配下に、端末やグループが表示されていることを確認します。



4) 画面上部の「管理」をクリックします。

5) 「管理」セクションの「Dr.Web Server」をクリックし、Dr.Web Server のバージョンを確認します。

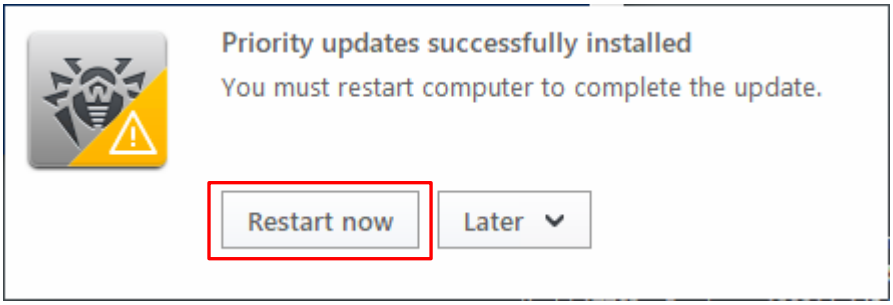
4.4 Agent の更新

Windows 用の Agent は、ESS12 に接続すると更新処理を自動的に開始します。Agent が更新された後、手動で OS を再起動する必要がありますので、注意してください。

1) ESS10 の Agent がインストールされた端末が ESS12 サーバに接続できるようにします。

2) ESS10 の Agent がインストールされた端末にログインします。

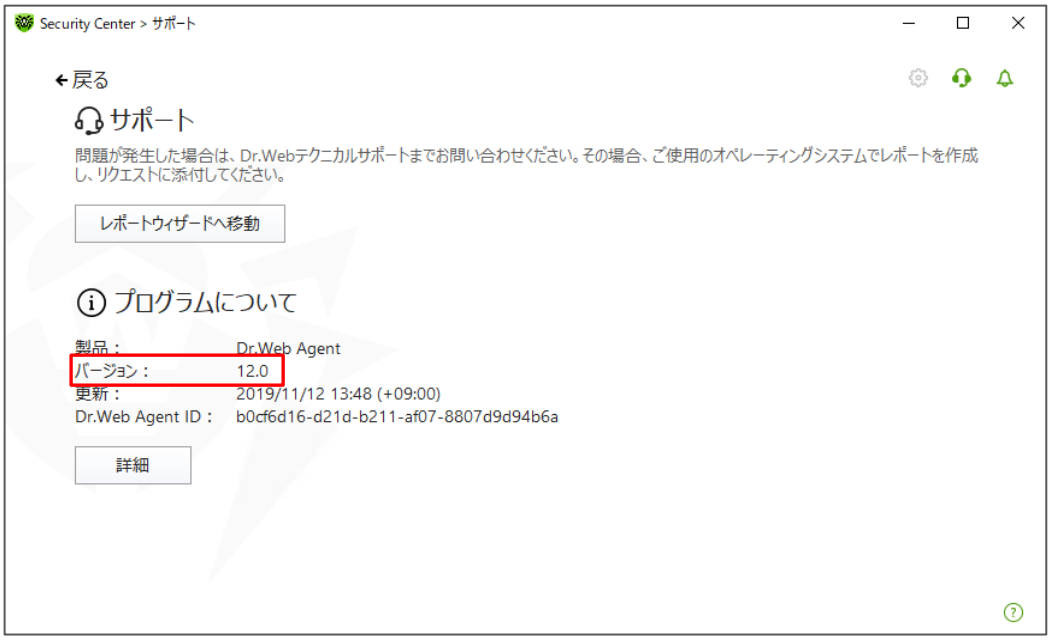
3) 以下のメッセージが表示されたら、「Restart now」をクリックします。



4) 端末を再起動し、再度ログインします。

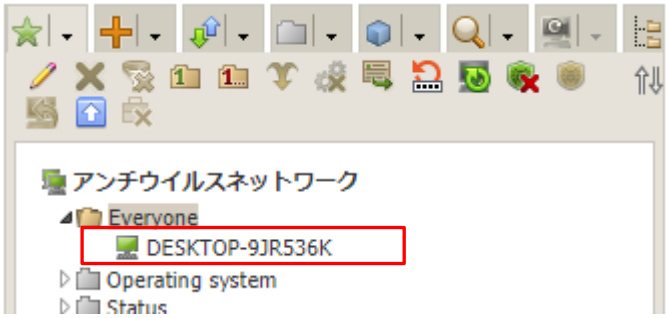
5) タスクバー上の Dr.Web の常駐アイコンを右クリックし、[ツール]-[サポート]をクリックします。

6) 以下のように「バージョン 12.0」と表示されていることを確認します。



7) CC にアクセスし、画面中央の「アンチウイルスネットワーク」ツリーの「Everyone」グループを開きます。

8) 端末の状態表示が、以下のように緑になっていることを確認します。



5. Control Center の設定

ESS サーバを使用するにあたっての設定を行ないます。

5.1 ESS サーバの更新【必須】

ESS サーバのアップデートの有無を確認し、アップデートがある場合には更新を行ないます。

1) CC にログインし、「管理」メニューを開き、「リポジトリの状態」をクリックします。
2) 「更新情報のチェック」ボタンをクリックし、最新のリポジトリを取得します。
3) リポジトリの更新完了後、「Dr.Web Server」をクリックし、「バージョンリスト」ボタンをクリックします。
4) アップデートがある場合、「全てのバージョン」の箇所に適用可能なものの一覧から、最新のものを選択し、「保存」ボタンをクリックします。
   ※ バージョン表記は、dd-mm-yyyy HH:mm:ss の形式です。
   ※ バージョンアップは、環境によって異なりますが、数分～数十分かかります。
5) バージョンアップ完了後、再度 CC にログインし、「管理」メニューで表示されている「Dr.Web Server のバージョン」が更新されたことを確認します。

※ ESS サーバのアップデートは不定期にリリースされます。メンテナンス等のタイミングでアップデートの有無を確認し、アップデートがある場合には更新を行なってください。

5.2 「Dr.Web Server の設定」の変更

5.2.1 サーバーアドレスの設定【必須】

1) CC にログインし、「管理」メニューを開き、「Dr.Web Server の設定」をクリックします。
2) 「ネットワーク」タブをクリックします。
3) 次に「ダウンロード」タブをクリックします。
4) 「Dr.Web Server アドレス」欄に、当該サーバの IP アドレス(または DNS 名)を入力します。
5) 「保存」をクリックし、設定を保存します。
6) 再起動要求が表示された場合、再起動ボタンをクリックして再起動します。

5.2.2 暗号化設定(サーバー側)の変更【推奨】

管理対象に Android 端末がある場合、以下の設定を行なってください。

1) CC にログインし、「管理」メニューを開き、「Dr.Web Server の設定」をクリックします。
2) 「ネットワーク」タブをクリックします。
3) 次に「トランスポート」タブをクリックします。
4) 「暗号化」の設定を、「はい」から「**可能であれば**」(もしくは、「**いいえ**」)に変更します。
5) 「保存」をクリックし、設定を保存します。
6) 再起動要求が表示された場合、再起動ボタンをクリックして再起動します。

5.2.3　Server 言語の変更【必須】

1) CC にログインし、「管理」メニューを開き、「Dr.Web Server の設定」をクリックします。
2) 「全般」タブをクリックします。
3) 「Server の言語」の設定を、「English」から「**日本語**」に変更します。
4) 「保存」をクリックし、設定を保存します。
5) 再起動要求が表示された場合、再起動ボタンをクリックして再起動します。

5.2.4　Server のログ設定の変更

ログレベル、保存する世代数、ログローテーションモード(時間またはサイズ)等を変更できます。
一定時間でのローテーションと保存する世代数の設定により、希望する期間のログを保存することができます。

1) CC にログインし、「管理」メニューを開き、「Dr.Web Server の設定」をクリックします。
2) 「ログ」タブをクリックします。
3) 必要に応じて、以下の設定を変更します。
   ※　下記は、初期値。
   Server ログの詳細レベル　：　トレース 3
   ファイル最大数　：　10
   Server ログローテーションモード：「指定したサイズでローテーション」
   各ファイルのサイズ上限　：　10MB
   ※　「指定した時間でローテーション」を選択した場合、ログのローテーション間隔(初期値は 10 時間)を指定可能です。
4) 「保存」をクリックし、設定を保存します。
5) 再起動要求が表示された場合、再起動ボタンをクリックして再起動します。

5.3 「Web サーバーの設定」の変更

5.3.1　サーバーアドレスの変更【必須】

1) CC にログインし、「管理」メニューを開き、「Web サーバーの設定」をクリックします。
2) 「全般」タブをクリックします。
3) 「Dr.Web Server アドレス」欄に、当該サーバの IP アドレス(または DNS 名)を入力します。
4) 「保存」をクリックし、設定を保存します。
5) 再起動要求が表示された場合、再起動ボタンをクリックして再起動します。

5.3.2　https へのリダイレクトの停止設定

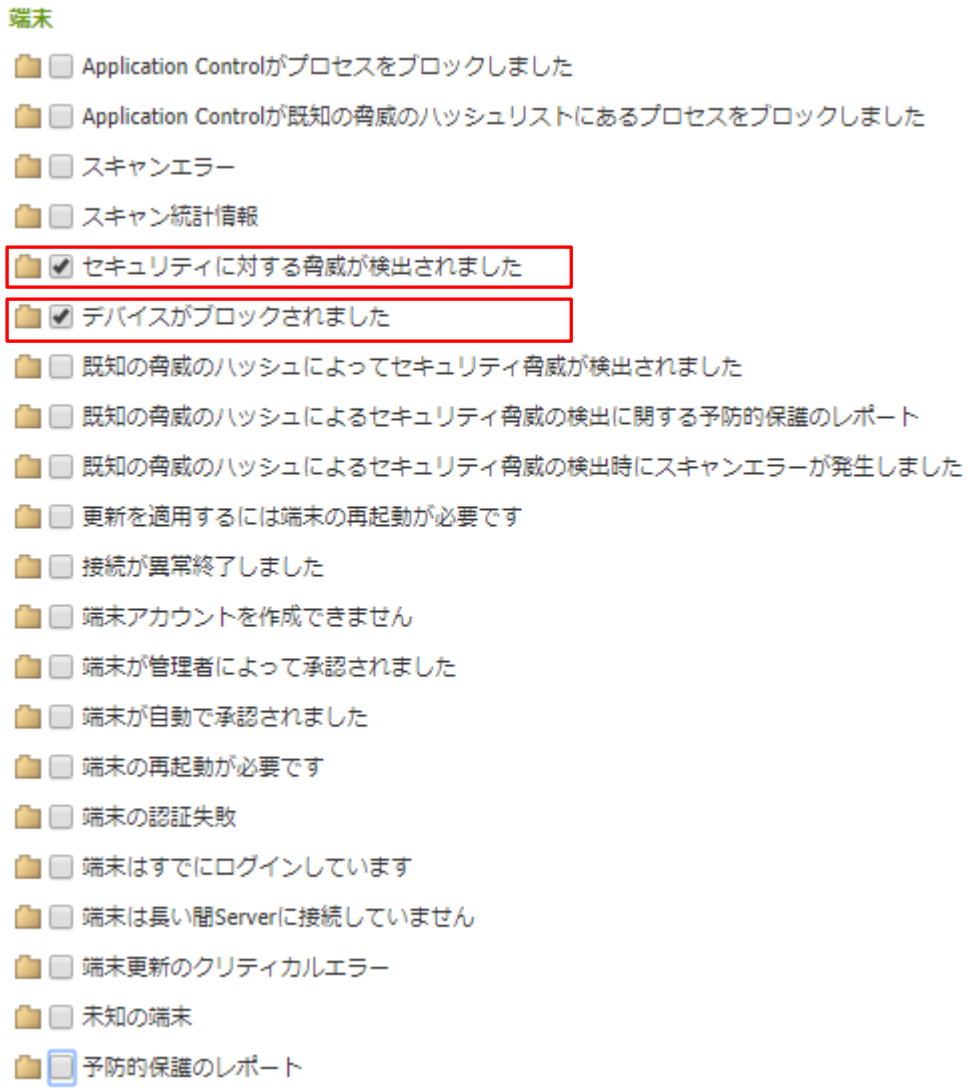
https へのリダイレクトを停止させる場合は、以下の設定を実施してください。

1) CC にログインし、「管理」メニューを開き、「Web サーバーの設定」をクリックします。
2) 「セキュリティ」タブをクリックします。
3) 「安全な接続にリダイレクトする」のチェックを外します。
4) 「保存」をクリックし、設定を保存します。
5) 再起動要求が表示された場合、再起動ボタンをクリックして再起動します。

5.4 「通知設定」の変更 **【推奨】**

初期状態では、管理者宛に多くの通知が行われ、その内容は DB 内に保存されます。これによりデータベースの肥大化が生じることもある為、端末に関する通知項目を「セキュリティに対する脅威が検出されました」のみに変更してください。

デバイス制御を使用されている場合には、必要に応じて「デバイスがブロックされました」も有効にしてください。



5.5 Dr.Web Agent 設定の変更

5.5.1 Dr.Web for MS Outlook の設定変更【必須】

MS Outlook 使用時に、メールに添付されているパスワードが設定された ZIP ファイル等が隔離されてしまうことを防止するため、以下の設定を行なってください。

【注意】"Dr.Web for MS Outlook"を「インストール不可」にしている場合でも、ライセンスの更新の際に自動的に「インストール可能」に変更されてしまう場合がありますので、"Dr.Web for MS Outlook"を使用するか否かに関わらず必ず以下の設定は実施してください。

1) CC にログインし、「アンチウイルスネットワーク」を開きます。
2) 画面中央のツリーから、「Everyone」グループを選択します。
3) 「Dr.Web for MS Outlook」をクリックします。
4) 「アクション」タブ内の「未検査ファイル」の設定を「隔離」から「**無視**」に変更します。
5) 「保存」ボタンをクリックします。

5.5.2 hosts の除外設定【推奨】

hosts の変更を行なっている環境において、Dr.Web により hosts が初期化される場合がありますので、これを防止するため、以下の設定を行なってください。

※ 入力された文字コードによっては、適切に動作しない場合があるため、本書記載の内容をコピーするのではなく、直接キーボードより入力してください。

1) CC にログインし、「アンチウイルスネットワーク」を開きます。
2) 画面中央のツリーから、「Everyone」グループを選択します。
3) 「Scanner」をクリックします。
4) 「除外」タブ内の「除外するパスとファイル」に以下を追加し、「保存」をクリックします。
   C:¥windows¥system32¥drivers¥etc¥hosts
5) 「SpIDer Guard for workstations」をクリックします。
6) 「除外」タブ内の「除外するパスとファイル」に以下を追加し、「保存」をクリックします。
   C:¥windows¥system32¥drivers¥etc¥hosts
7) 「SpIDer Guard for servers」をクリックします。
8) 「除外」タブ内の「除外するパスとファイル」に以下を追加し、「保存」をクリックします。
   C:¥windows¥system32¥drivers¥etc¥hosts

5.5.3　Windows8、Windows10 使用時の設定変更【推奨】

Windows8 や Windows10 を使用している場合、Dr.Web からの通知(再起動要求、脅威の検出等)が一切表示されない場合があります。その場合、以下の設定を行なってください。

1) CC にログインし、「アンチウイルスネットワーク」を開きます。
2) 画面中央のツリーから、「Everyone」グループを選択します。
3) 「Dr.Web Agent」をクリックします。
4) 「インターフェース」タブ内の「フルスクリーンモードの時には通知を表示しない」のチェックを外します。
5) 「保存」ボタンをクリックします。

6. Agent の追加

既存の Agent に加え、新規で Windows PC に Agent をインストールする場合、コンポーネントの選択の後、本項の手順にて配布、インストール、承認を行なってください。

6.1 Agent のインストールの前に

6.1.1 導入するコンポーネントの選択

Agent は複数のコンポーネントから構成され、コンポーネント単位でインストールするか否かを選択できます。必要に応じて、CC 上で[アンチウイルスネットワーク]-[インストールするコンポーネント]からインストールするコンポーネントを選択してください。初期状態では以下となっており、ライセンスの種類にかかわらず”Dr.Web Firewall”はインストールされません。

※ “SpIDer Guard for Windows workstations”と”SpIDer Guard for Windows Severs”につきましては、OS の種類(クライアント OS かサーバ OS)により、どちらかがインストールされます。

また、**Windows Server に対しては、以下のコンポーネント以外は導入しないでください。**

- Dr.Web Agent for Windows
- Dr.Web Scanner
- Dr.Web Scanner for Windows
- SpIDer Guard for Windows Servers

6.1.2　その他注意事項等

6.1.2.1.　インストール時に使用するユーザ名について

Agent のインストール時に使用するユーザ名が全角で 17 文字以上の場合、インストールに失敗する場合があります。この場合は、インストール用に短い名前のユーザを追加していただき、追加したユーザでインストールを実施してください。

6.1.2.2.　環境復元ソフトがインストールされている場合

環境復元ソフトがインストールされている場合、環境復元ソフトを停止した状態(復元機能が実行されない状態)でインストールを実施してください。また、予め Control Center の更新の設定を「ウイルスデータベースのみ」に変更して、クライアントの Windows PC にインストールされた Dr.Web Agent のコンポーネントが変更されない様にしてください。

この設定変更は、以下の 2 つの方法があります。

1) 「管理」メニューの[レポジトリー般設定]-[Dr.Web Agent]を開き、「Dr.Web Agent for Windows」タブから

   この設定では、管理サーバ(Control Center)自体に更新された Windows 用の Dr.Web Agent のコンポーネントがダウンロードされませんので、当該 Control Center で管理される全ての Dr.Web Agent for Windows のコンポーネントは更新されません。

2) 「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対象のグループ(または端末)を選択後、「更新の制限」を開き、「更新制限」から

   この設定では、管理サーバ(Control Center)自体に更新された Windows 用の Dr.Web Agent のコンポーネントがダウンロードされますが、更新制限が設定されたグループ(または端末)のみ Dr.Web Agent for Windows のコンポーネントが更新されません。

   ※　更新制限が設定されていないグループ(または端末)の Dr.Web Agent for Windows のコンポーネントは更新されます。

また、正常に定義ファイルの更新が行われている状況においても「Dr.Web ウイルスデータベースが最新ではありません」、「コンピューターが脅威に晒される可能性があります」等のメッセージが表示されることがありますが、実際にはディスク内の定義ファイルが読み込まれております。

ディスク内の定義ファイルの状態につきましては、Dr.Web の常駐アイコンをクリックして表示されたメニューの[サポート]をクリックし、表示されたウィンドウに表示された「ウイルスデータベース」よりご確認ください。

※　drwtoday.vdb の日付をご確認ください。

6.1.2.3.　URL フィルタリングソフトがインストールされている場合

URL フィルタリングソフトがインストールされている場合、ホームページの閲覧等ができなくなる場合があります。その際は、SpIDer Mail、SpIDer Gate、Dr.Web for MS Outlook をアンインストールしてください。

6.1.2.4.　管理下の OS に Windows Server と Windows クライアント(Windows10 等)が混在する場合

Dr.Web Agent for Windows のコンポーネント更新により、OS の再起動が必要となる場合があります。Windows Server については、利用の目的によっては再起動が制限されると思いますので、定義ファイルのみの更新とし、メンテナンス等のタイミングでコンポーネントの更新をしてください。

設定方法については、6.1.2.2 の 2)を参照ください。

6.1.2.5.　レガシーファイルシステムフィルタードライバーを用いるアプリケーションがインストールされている場合

レガシーファイルシステムフィルタードライバーを使用するアプリケーションがインストールされている環境に、Dr.Web Agent for Windows をインストールした場合にブルースクリーンが発生し、OS が起動しない場合があります。レガシーファイルシステムフィルタードライバーを使用するアプリケーションがインストールされている環境では、Dr.Web Agent for Windows のインストールを実施する前に、Control Center 上で予防的保護の「ディスクへの低レベルアクセス」を「ブロック」から「許可」に変更してください。

6.2 Agent のインストーラの配布とインストール、承認

6.2.1 Agent のインストーラの配布

Agent のインストーラと証明書を、以下の URL よりダウンロードし、Dr.Web をインストールする端末に配布してください。また、Agent インストーラと証明書は、インストールする端末上の同じフォルダに保存してください。

- Agent のインストーラ

  URL　　：　https://<ESS サーバの IP アドレス or DNS 名>:9081/install/windows

  　　http://<ESS サーバの IP アドレス or DNS 名>:9080/install/windows

  ファイル名　：　drwinst.exe

- 証明書

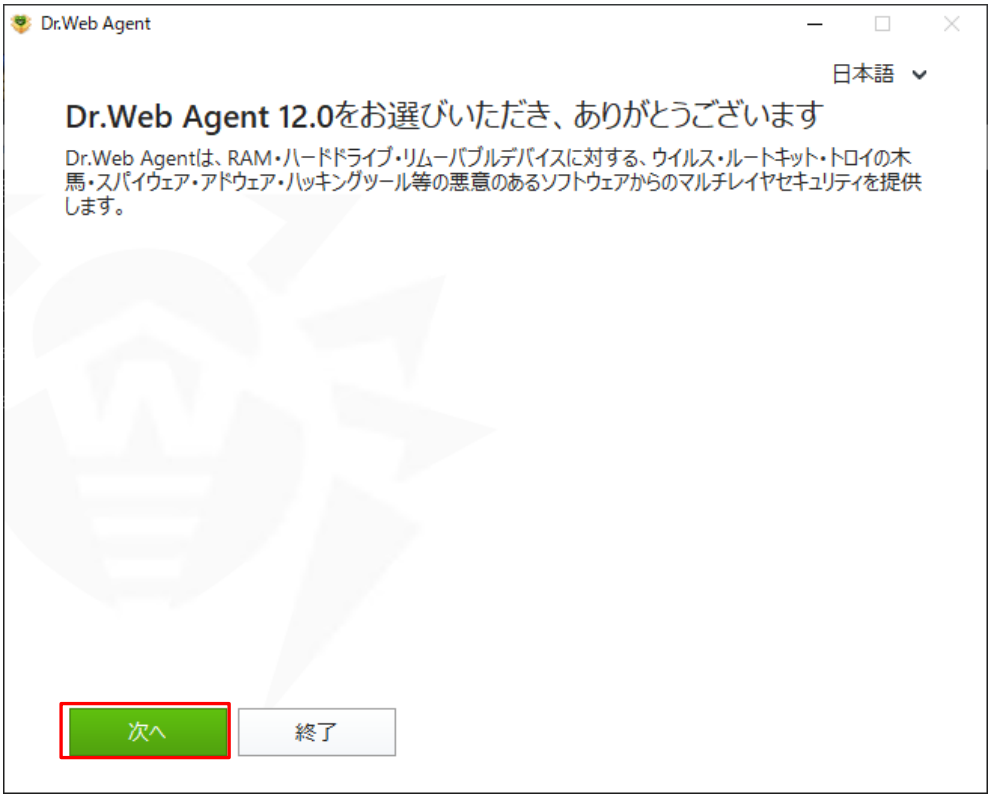
  URL　　：　https://<ESS サーバの IP アドレス or DNS 名>:9081/install/windows

  　　http://<ESS サーバの IP アドレス or DNS 名>:9080/install/windows

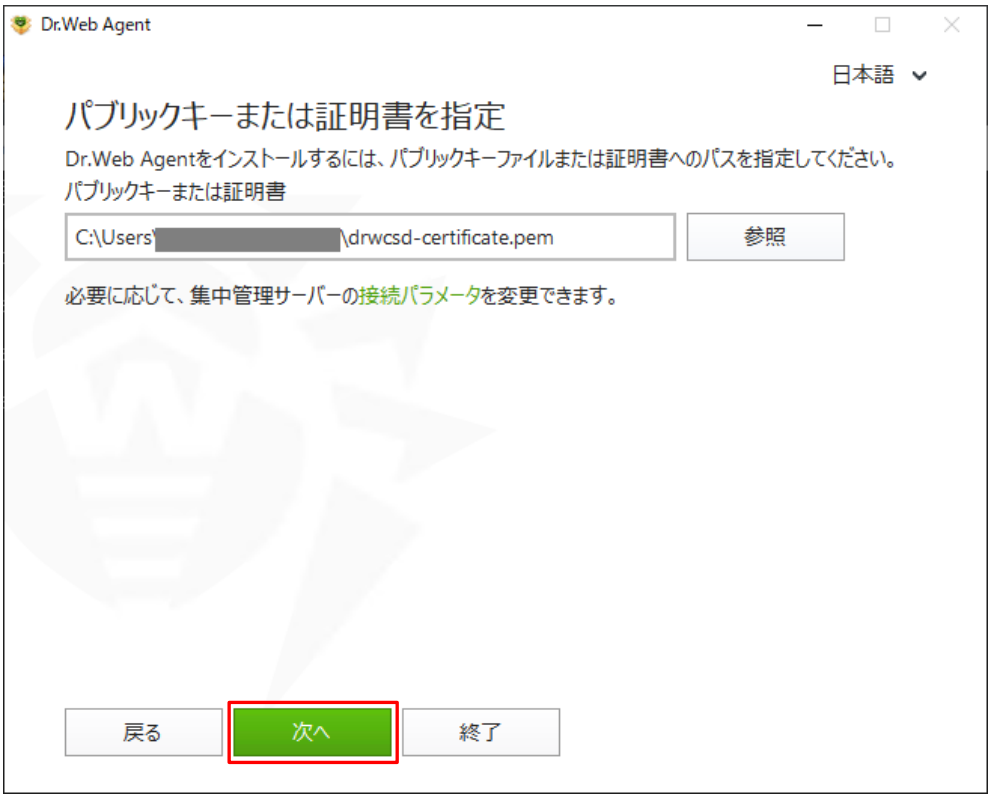
  ファイル名　：　drwcsd-certificate.pem

6.2.2 Agent のインストール、承認

1) 端末上に保存した Agent のインストーラ(drwinst.exe)を実行します。
2) 以下の画面が表示されたら、「次へ」をクリックします。

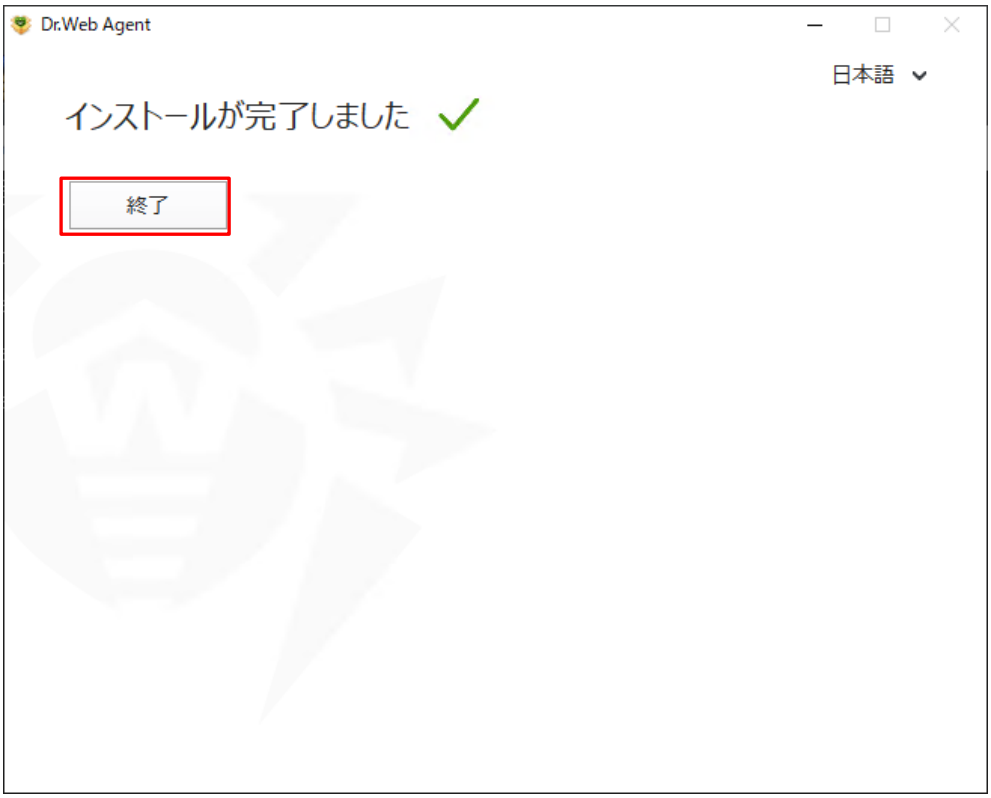


3) 以下の画面で暗号化キーが指定されていることを確認して、「次へ」をクリックします。



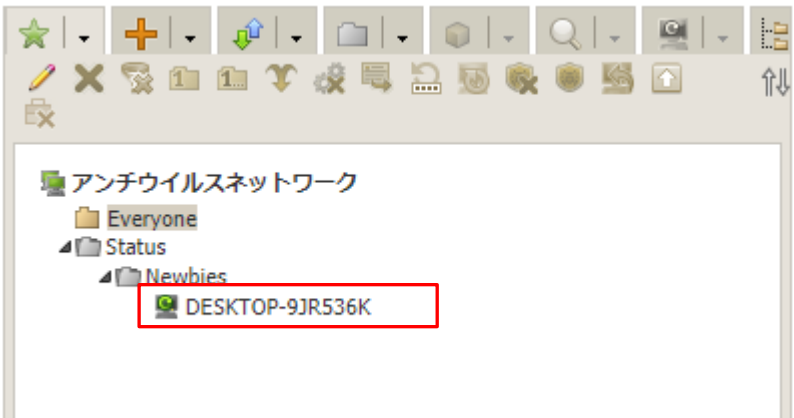
4) しばらくすると、以下の画面が表示されるので、「インストール」をクリックします。

5) 以下の画面が表示されたら、「終了」をクリックします。

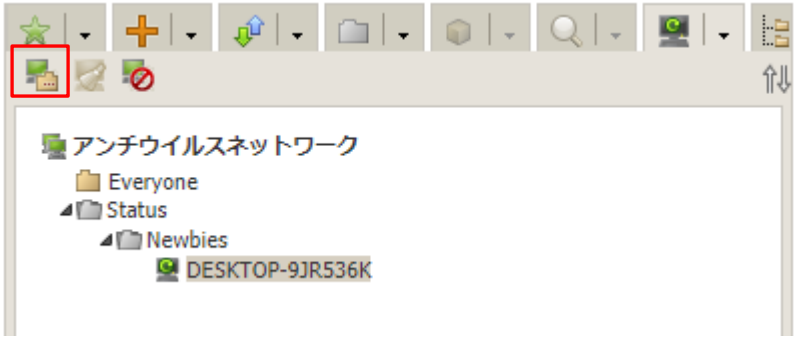


6) CC にログインし、「アンチウイルスネットワーク」メニューを開きます。

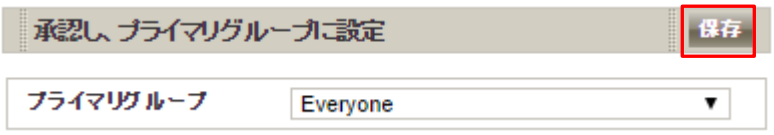
7) 画面中央のツリーから、[Status]-[Newbies]を開き、インストールした端末が表示されていることを確認します。



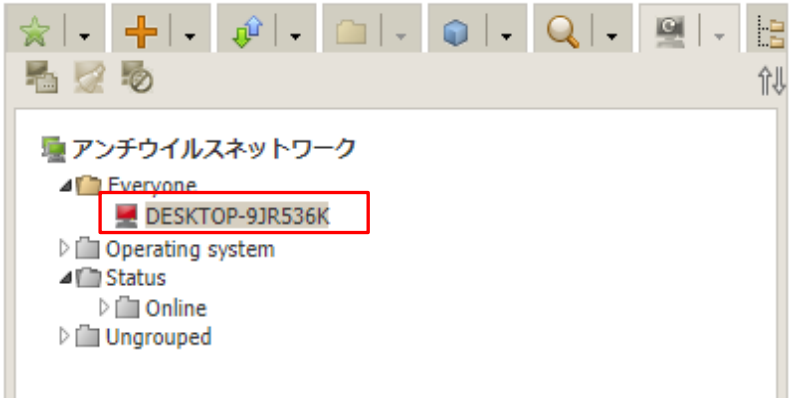
8) インストールした端末(以下の図では、DESKTOP-9JR536K)を選択し、「選択した端末を承認し、プライマリグループを設定」ボタンをクリックします。



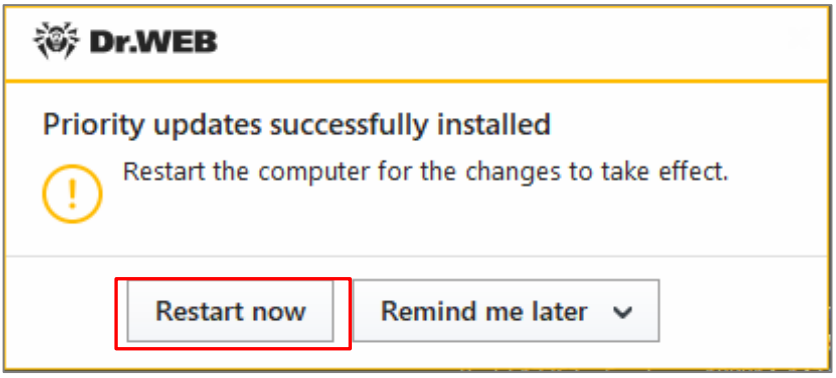
9) 画面右側から「プライマリグループ」を選択し、「保存」ボタンをクリックします。



10) 画面中央のツリーの「Everyone」グループに承認した端末が表示されたことを確認します。



11) 端末を承認した後、しばらくすると Agent をインストールした端末上に以下のメッセージが表示されるので、「Restart now」をクリックします。



6.3 その他の Agent のインストール方法

Agent のインストールは、上記 6.2 の方法以外に、端末毎の専用インストーラ、グループ専用インストーラ、Windows OS 向けエージェントインストーラーフルパッケージ、Active Directry によるログオンスクリプト等の様々な方法で実施することができます。

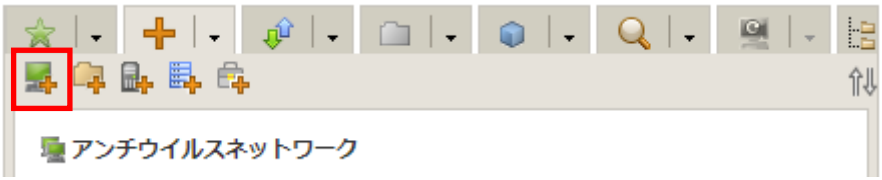
6.3.1 端末毎の専用インストーラ

端末(Agent)毎に専用のインストーラを作成しますので、これを用いると、サーバ上での承認が不要となります。また、インストール完了時には、再起動要求が表示されます。

※ インストーラには、端末 ID(Agent ID)等が含まれる為、インストール時の承認は不要ですが、端末 ID が重複する為、異なる PC に対して同じインストーラを使用することはできません。

1) CC にログインし、「アンチウイルスネットワーク」メニューを開きます。
2) 中央のツリーの「＋」のボタンをクリックします。

3) 次にモニタのアイコンをクリックします。



4) 「新規端末」の箇所で、パスワードを入力し、「保存」をクリックします。

※ 必要に応じてプライマリグループの設定を行なってください。

5) 「インストールファイル」の”Windows”をクリックし、専用インストーラをダウンロードします。

6) ダウンロードした専用インストーラ(drweb_ess_windows_<名前>.exe)をインストール対象に PC にコピーした後、実行します。

※ 証明書(drwcsd-certificate.pem)は専用インストーラに含まれるので、別途用意する必要はありません。

※ 以降は画面の表示に従って進めてください。

7) インストールが完了したら、PC の再起動を実施します。

6.3.2 グループ毎の専用インストーラ

グループ毎に専用のインストーラを作成します。これを用いると、端末毎の専用インストーラと同じように、サーバ上での承認が不要となり、また自動的に当該グループがプライマリグループとして設定されます。インストール完了後には、再起動を実施してください。

※ Everyone グループ用の専用インストーラは作成できません。

※ インストール時の承認は不要です。

1) CC にログインし、「管理」メニューを開きます。

2) [Dr.Web Server の設定]-[全般]を開きます。

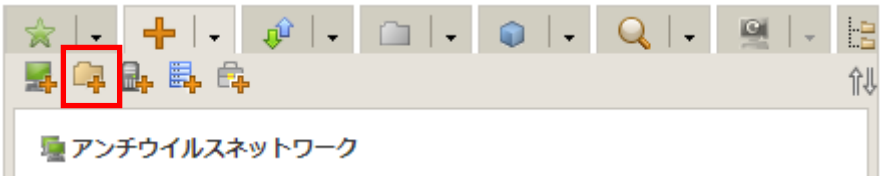
3) 「端末アカウントを自動的に作成する」のチェックを入れ、保存をクリックします。

※ 再起動要求が表示された場合、再起動ボタンをクリックして再起動してください。

4) 「アンチウイルスネットワーク」メニューを開きます。

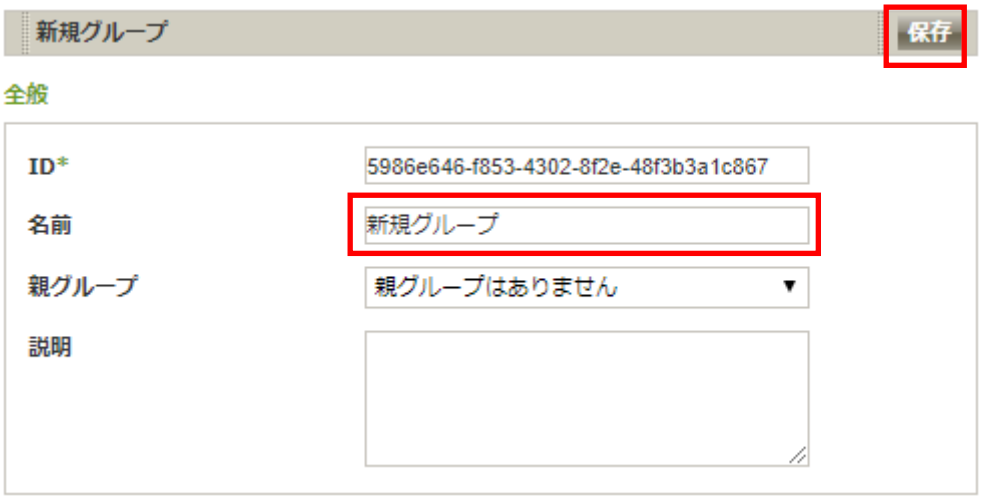
5) 中央のツリーの「＋」のボタンをクリックします。

6) 次にフォルダのアイコンをクリックします。



7) 「新規グループ」の箇所で、名前を入力し、「保存」をクリックします。

※ 必要に応じて親グループを指定してください。



8) 中央のツリーに新規グループが追加されたことを確認します。

9) 追加された新規グループを選択します。

10) グループのプロパティの画面から、「インストールファイル」の"Windows"をクリックし、グループ専用インストーラをダウンロードします。

11) ダウンロードした専用インストーラ(drweb_ess_windows_<グループ名>.exe)をインストール対象に PC にコピーした後、実行します。

※ 証明書(drwcsd-certificate.pem)は専用インストーラに含まれるので、別途用意する必要はありません。

※ 以降は画面の表示に従って進めてください。

12) インストールが完了したら、PC の再起動を実施します。

6.3.3　Windows OS 向けエージェントインストーラーフルパッケージ

作成日時点での全てのコンポーネントおよび定義ファイルが含まれたインストーラです。これを用いることにより、他の方法と比較して、インストール時の Agent-サーバ間のトラフィックを抑えることができます。

1) 弊社ダウンロードサイトより Windows OS 向けエージェントインストーラーフルパッケージをダウンロードします。

※　2019/11/15 時点では、Ver10 用および Ver11 用の Windows OS 向けエージェントインストーラーフルパッケージもダウンロード可能なため、バージョンに注意してください。

2) ダウンロードした Windows OS 向けエージェントインストーラーフルパッケージと証明書(drwcsd-certificate.pem)をインストールする PC の同じフォルダにコピーした後、実行します。

※　以降は画面の表示に従って進めてください。

3) インストールが完了したら、PC の再起動を実施します。

4) PC の再起動中に 6-1-2 の 6)～10)の手順を実行します。

※　必ず、端末を CC 上で承認してください。

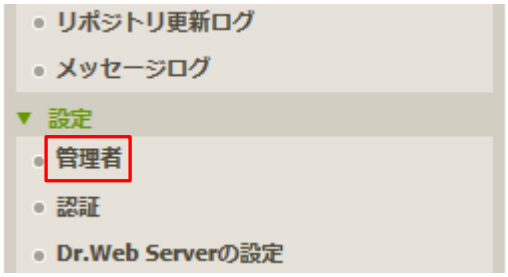
7. ケーススタディ

7.1 管理者(admin)パスワードの変更

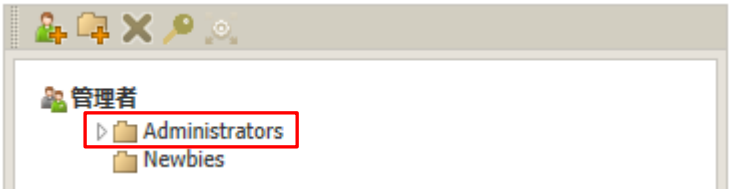
1) CC にログインします。

2) 「管理」メニューに移動します。

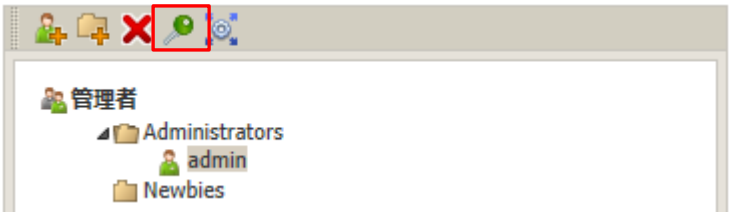
3) [設定]-[管理者]をクリックします。



4) 画面中央のツリーから「Administrators」を展開します。

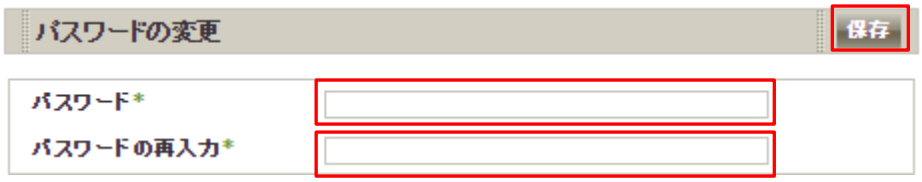


5) 「admin」を選択し、「パスワードの変更」アイコンをクリックします。



※ 「admin」を選択した後、「パスワードの変更」アイコンがクリックできるようになります。

6) パスワードを入力し、「保存」ボタンをクリックします。



7) 一度ログアウトし、変更したパスワードでログインできるか確認します。

7.2 ライセンスの更新

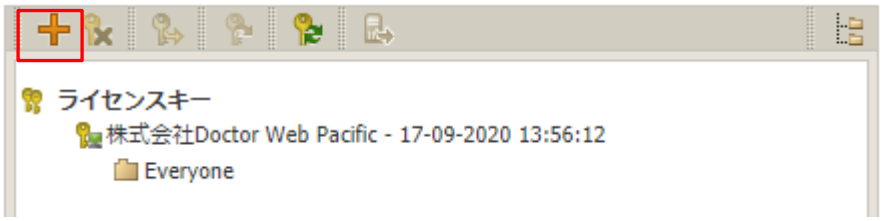
ライセンスキーは、基本的には「Everyone」グループに紐づけてください。

※ ESS12 では、ESS10 や ESS11 と同様に一つのグループに複数のライセンスキーを紐づけたり、逆に一つのライセンスキーに複数のグループを紐づけたりすることが可能です。ライセンスキーとグループは、1 対 1 ではなく、n 対 n の関係となります。

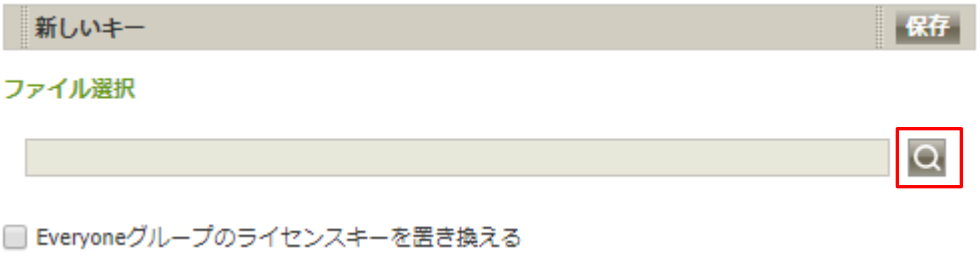
※ 複数のライセンスがある場合、Everyone グループに割り当てたライセンス以外を特定のグループに紐づけることも可能です。ライセンスが紐づけられたグループをプライマリグループとして設定されている端末に、配信されます。

1) CC にログインします。
2) 「管理」メニューに移動します。
3) [設定]-[ライセンスマネージャー]をクリックします。

4) 画面中央の「ライセンスキー」と書かれたツリーの上にある「ライセンスキーの追加」アイコンをクリックします。

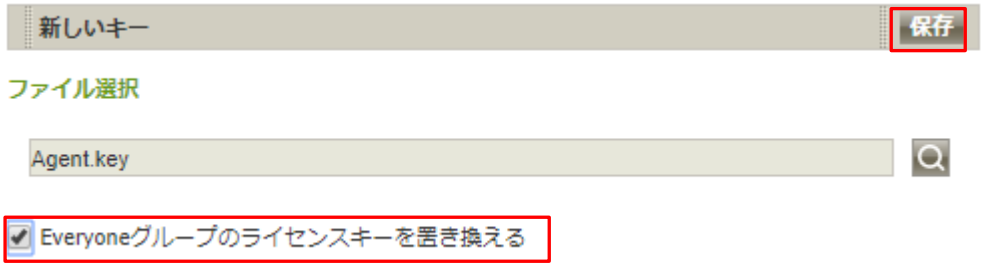


5) 画面右側に表示された虫眼鏡のアイコンをクリックします。



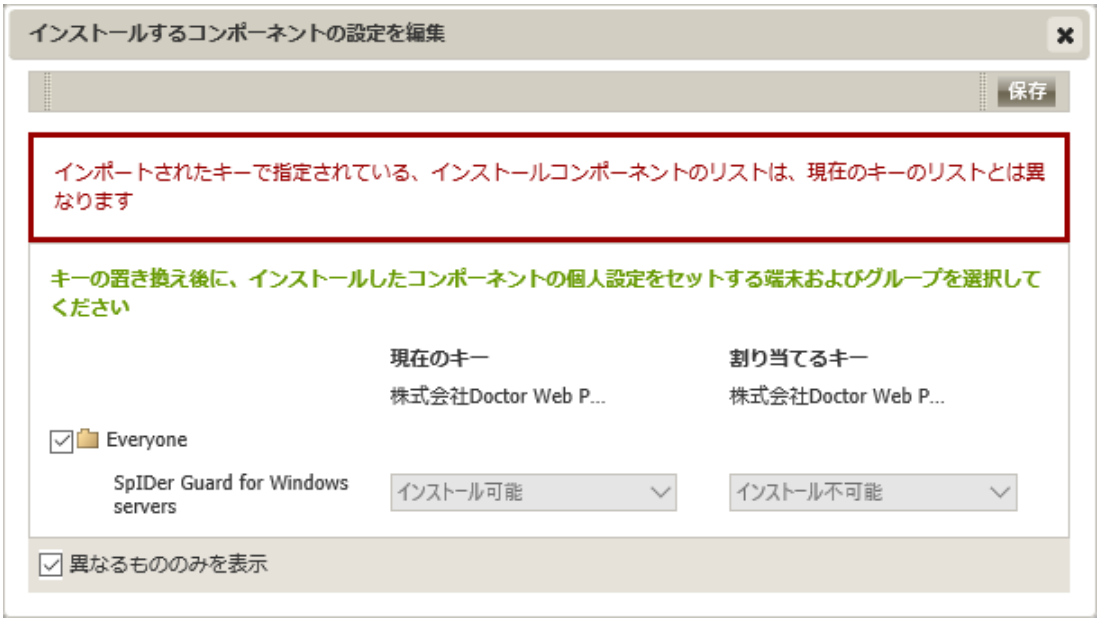
6) 新しいライセンスの Agent.key を指定し、「開く」をクリックします。

7) 「Everyone グループのライセンスキーを置き換える」にチェックを入れ、「保存」ボタンをクリックします。

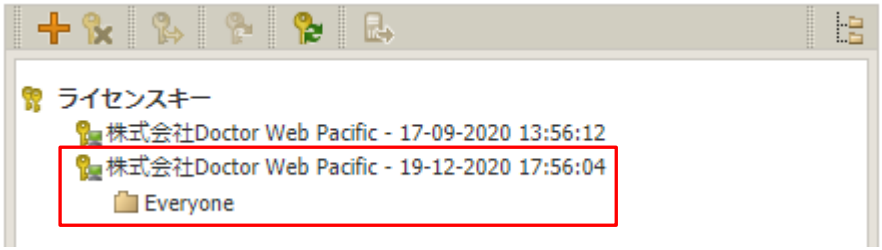


8) 以下のような画面が表示され、新旧のライセンスで使用可能なコンポーネントに差異が無いことを確認し、「保存」をクリックします。

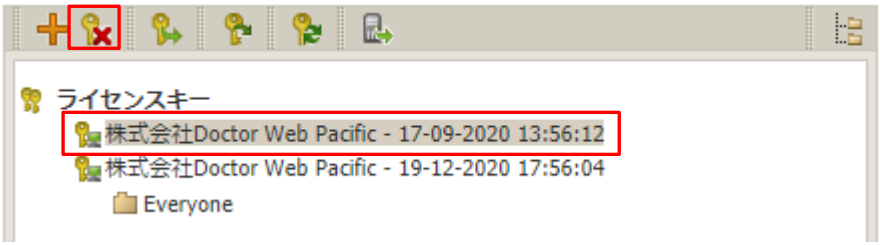
※ 以下のような表示は、現在のライセンスと新しいライセンスで利用可能なコンポーネントが異なることを表しています。



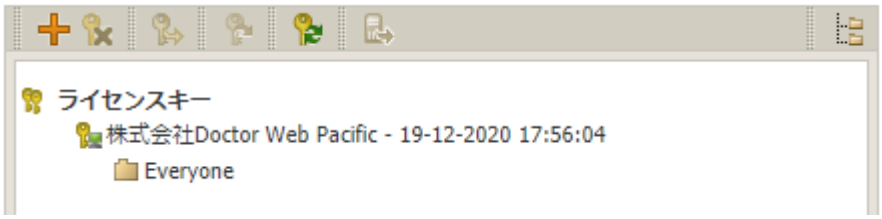
9) 画面中央の「ライセンスキー」ツリーに追加したライセンスの「登録名」と「ライセンス終了日」が表示されたこと、「Everyone」グループが紐づいたことを確認します。



10) 以前のライセンスキーを選択し、「選択したオブジェクトの削除」ボタンをクリックします。



11) 以前のライセンスキーが削除されたことを確認します。



※ 「インストールするコンポーネント」の設定を変更している場合、その設定が変更されていることがありますので、必ずライセンス更新後に「インストールするコンポーネント」の設定を確認してください。

7.3 Agent のインストールに失敗する

Agent のインストールに失敗する場合、下記を確認後、再度実行してください。

- ESS サーバが起動しているか
- インストール時に指定した証明書(drwcsd-certificate.pem)が、接続する ESS サーバのものか
- ESS サーバ、Agent をインストールする端末で必要なポートが解放されているか
- ネットワーク機器により、ESS サーバと Agent 間で使用するポートが閉じられていないか

再度実行しても失敗する場合は、以下のようにコマンドラインから接続する ESS サーバを指定して実行してください。

例) drwinst.exe と drwcsd-certificate.pem を「C:¥temp」フォルダに保存している場合

```
C:¥temp> drwinst.exe /server <ESS サーバの IP アドレス>
```

7.4 Dr.Web Agent for Windows の言語の変更

初期状態では、「システム言語」が設定されておりますが、クライアント上の Dr.Web のメニュー等の表示が全て英語で表示されている場合には、以下の手順で OS の言語と同じもので表示されるように変更してください。

1) CC にログインし、「アンチウイルスネットワーク」を開きます。
2) 画面中央のツリーから、「Everyone」グループを選択します。
3) 「Dr.Web Agent」をクリックします。
4) 「全般」タブの「言語」の設定を「English」から「システム言語」に変更します。
5) 「保存」ボタンをクリックします。

7.5 端末の追加に失敗する

CC 上で、「ネットワーク」メニューから端末の追加を行なった際に、下記のようなメッセージが表示される場合があります。

この場合は、次の事項を確認してください。

- Agent.key が登録されているか
- 有効な Agent.key が「Everyone」グループに配信されているか
- ライセンスで許可された数量の端末が、既に Everyone グループ内に表示されていないか

7.6 hosts ファイルを変更するアプリケーションのインストール

アプリケーションのインストール時に hosts ファイルを変更するもの(例えば、VMware Horizon View Client 等)をインストールされる場合、予防的保護により hosts ファイルの変更がブロックされアプリケーションのインストールに失敗します。

このようなアプリケーションをインストールされる場合は、以下を無効化(停止)した状態でインストールを実施してください。

- セルフプロテクション
- 予防的保護

7.7 スケジュールスキャン設定時の注意事項

「アンチウイルスネットワーク」メニューの「Task Scheduler」からスケジュールスキャンを登録することができます。しかしながら、Task Scheduler で Dr.Web Scanner によるスキャンジョブ(フルスキャン、クイックスキャン、カスタムスキャン)を設定した場合、Scaner の個所で設定した内容は反映されず、除外等しているファイルに対してもスキャンが実施されます。

そのため、スケジュールスキャンを設定される際は、**カスタムスキャンを選択**し、手動で除外設定を行ってください。

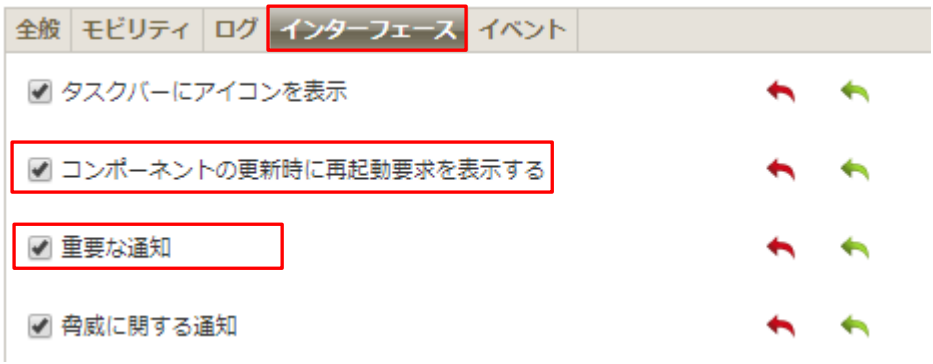
7.8 リポジトリの更新による PC の再起動を止めたい

Agent プログラムの更新により、PC の再起動を要求されることがあります。以下の方法で、再起動要求を表示せず、自動的に再起動がされないようにすることができます。また、この方法では、手動で PC の再起動を実施することにより、更新プログラムが適用されます。

※ 「高速スタートアップ」が有効になっている場合、PC のシャットダウンおよび起動では更新プログラムは適用されません。

1) CC にログインします。
2) 「アンチウイルスネットワーク」メニューを開きます。
3) 画面中央のツリーの「Everyone」グループを選択します。
   ※ 全ての端末ではなく特定の端末や特定のグループに対して設定したい場合は、該当の端末もしくはグループを選択してください。
4) 画面右側の「設定」セクションから[Windows]-[Dr.Web Agent]をクリックします。

5) 中央に表示されたメニューから、「インターフェース」を選択し、「コンポーネントの更新時に再起動要求を表示する」と「重要な通知」のチェックを外します。



6) 「保存」ボタンをクリックし、設定を保存します。

7.9 PC のクローニングについて

sysprep で作成した OS のマスターイメージをクローニングして展開する場合、構築済み ESS サーバとの通信可否により、手順が異なります。証明書が必要となるため、ESS サーバの構築が完了していない状態では、マスターイメージに含めることはできません。

また、ESS サーバの IP アドレス等は、マスターイメージ作成時とクローニング後で変更がないことが前提となります。

7.9.1 構築済みの ESS サーバがあり、イメージ展開時に通信が可能な場合

マスターイメージに含むことが可能ですが、未承認の端末となる為、ミニセットアップ完了後に CC 上で承認が必要になります。SetupComplete.cmd につきましては、MS 社 HP にてご確認ください。また、本番運用を行なう前に必ず動作検証を行なってください。

7.9.1.1. drwinst.exe を使用する場合

drwinst.exe は最小限のパッケージとなり、ESS サーバにて承認された後、インストールに必要なファイルや定義ファイルをダウンロードしインストールを行います。

1) drwinst.exe と drwcsd-certificate.pem をマスター作成用 PC の同じフォルダに保存します。
2) ミニセットアップ完了後に、以下のコマンドが実行されるように SetupComplete.cmd で指定します。

drwinst.exe /silent yes /server <ESS サーバの IP アドレス> /pubkey <drwcsd-certificate.pem へのパス>

※ “/silent yes“を指定することにより、インストーラ実行中の画面が表示されません。

例)drwinst.exe と drwcsd-certificate.pem が「C:¥temp」に保存されており、ESS サーバの IP アドレスが 192.168.1.146 の場合

C:¥temp¥drwinst.exe /silent yes /server 192.168.1.146 /pubkey C:¥temp¥drwcsd-certificate.pem

3) Sysprep を実行します。
4) クローン PC を作成します。
5) クローン PC を起動し、ミニセットアップを実行します。
6) CC にログインし、「アンチウイルスネットワーク」メニューを開きます。
7) 画面中央のツリーから、[Status]-[Newbies]を開きます。
8) 表示されている端末を選択し、「選択した端末を承認し、プライマリグループを設定」ボタンをクリックします。
9) グループを選択し、「保存」ボタンをクリックします。
10) クローン PC のタスクトレイ上に、Dr.Web のアイコンが表示されたら、再起動します。

7.9.1.2. Windows OS 向けエージェントインストーラーフルパッケージを使用する場合

Windows OS 向けエージェントインストーラーフルパッケージには、インストールに必要なファイルが全て含まれております。インストール完了後、ESS サーバにて承認された後に定義ファイルをダウンロードします。

1) Windows OS 向けエージェントインストーラーフルパッケージを、Dr.Web の HP よりダウンロードします。
2) ダウンロードしたインストーラと drwcsd-certificate.pem をマスター作成用 PC の同じフォルダに保存します。
3) ミニセットアップ完了後に、以下のコマンドが実行されるように SetupComplete.cmd で指定します。

drweb-12.00.0-201910280-esuite-agent-full-windows.exe /silent yes /server <ESS サーバの IP アドレス>

※ インストーラの数字部分は、異なる場合があります。

※ "/silent yes"を指定することにより、インストーラ実行中の画面は表示されません。

例)インストーラと drwcsd-certificate.pem が「C:¥temp」に保存されており、ESS サーバの IP アドレスが 192.168.1.146 の場合

C:¥temp¥drweb-12.00.0-201910280-esuite-agent-full-windows.exe /silent yes /server 192.168.1.146

4) Sysprep を実行します。
5) クローン PC を作成します。
6) クローン PC を起動し、ミニセットアップを実行します。
7) CC にログインし、「アンチウイルスネットワーク」メニューを開きます。
8) 画面中央のツリーから、[Status]-[Newbies]を開きます。
9) 表示されている端末を選択し、「選択した端末を承認し、プライマリグループに設定」ボタンをクリックします。
10) グループを選択し、「保存」ボタンをクリックします。

7.9.2 構築済みの ESS サーバがあり、イメージ展開時に通信が不可能な場合

ESS サーバと通信が可能となった状態で、各 PC から Agent のインストールを実行してください。

構築済みの ESS サーバがあるので、予めインストーラ(drwinst.exe もしくは Windows OS 向けエージェントインストーラーフルパッケージ)と証明書(drwcsd-certificate.pem)を HDD 内に保存した状態でのマスターイメージの作成は可能です。

7.9.3 構築済みの ESS サーバがない場合

ESS サーバを構築後に、各 PC に Agent をインストールしてください。

7.10業務用のアプリケーションが脅威として検知された場合の対処

業務用アプリケーションが脅威として検知された場合、検知されたファイルを下記 URL より弊社にご送付ください。弊社にて確認後、誤検知であった場合には、検出されないよう対処します。

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

※　プログラムのバージョン等が変更となった後、再度検出された場合は、当該ファイルをお送りください。

上記の弊社対応には時間をいただきますので、ファイルを弊社にお送りいただくとともに以下の設定を行なっていただけますようお願いいたします。

- SpIDer Guard の除外設定
  1) CC にログインします。
  2) 「アンチウイルスネットワーク」メニューから、「Everyone」グループを選択します。
  3) SpIDer Guard for workstations をクリックします。
     ※　Windows Server に対して設定する場合は、SpIDer Guard for servers をクリックしてください。
  4) 「除外」をクリックし、”**除外するパスとファイル**”および”**除外するプロセス**”に当該ファイルをフルパスで指定します。
  5) 「保存」をクリックします。

- Dr.Web Scanner の除外設定
  1) CC にログインします。
  2) 「アンチウイルスネットワーク」メニューから、「Everyone」グループを選択します。
  3) Scanner をクリックします。
  4) 「除外」をクリックし、”**除外するパスとファイル**”に当該ファイルをフルパスで指定します。
  5) 「保存」をクリックします。

7.11 業務用のアプリケーションの起動等が遅くなった場合の対処

業務用アプリケーションの起動等が明らかに遅くなった場合、SpIDer Guard によるリアルタイムスキャンが影響している可能性があります。

その場合は、以下の設定を行なっていただけますようお願いいたします。

1) CC にログインします。
2) 「アンチウイルスネットワーク」メニューから、「Everyone」グループを選択します。
3) SpIDer Guard for workstations をクリックします。
   ※ Windows Server に対して設定する場合は、SpIDer Guard for servers をクリックしてください。
4) 「除外」をクリックし、該当する実行ファイルやフォルダを指定します。
   "**除外するプロセス**" : 起動等が遅くなったアプリケーションの実行ファイル等を指定
   ※ 複数ある場合は、複数の実行ファイルをフルパスで指定してください。
   "**除外するパスとファイル**" : 起動等が遅くなったアプリケーションのワークフォルダ、テンポラリフォルダやログファイル等を指定
5) 「保存」をクリックします。

≪事例≫

事　象 : Dr.Web Agent インストール後から、TWAIN ドライバを使用しているスキャナの取り込みが非常に遅くなった。

原　因 : スキャナ取り込み時に TWAIN.LOG ファイルが更新されるが、その更新の都度 SpIDer Guard によるスキャンが実行される為。

対　処 : TWAIN.LOG ファイルを SpIDer Guard の"**除外するパスとファイル**"に登録します。

登録例 : C:¥Users¥*¥AppData¥Local¥Temp¥TWAIN.LOG

※ Windows7 や Windows8 の場合

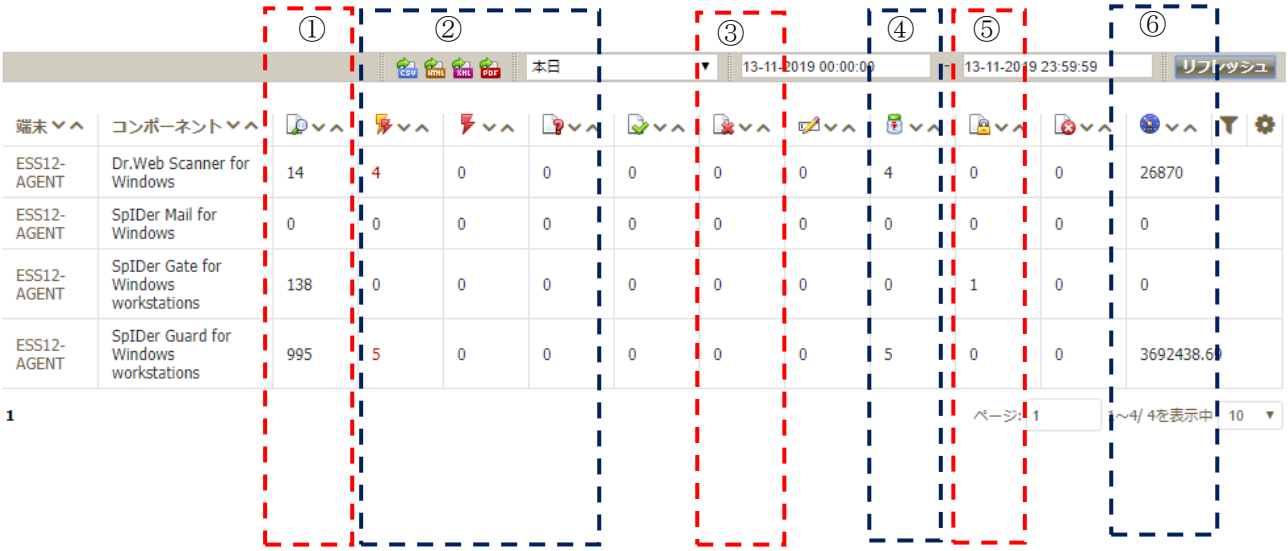
7.12統計情報

7.12.1　スキャン統計情報

「スキャン統計情報」から指定した期間における、選択したグループに含まれる端末のコンポーネント毎に以下の内容を確認することができます。

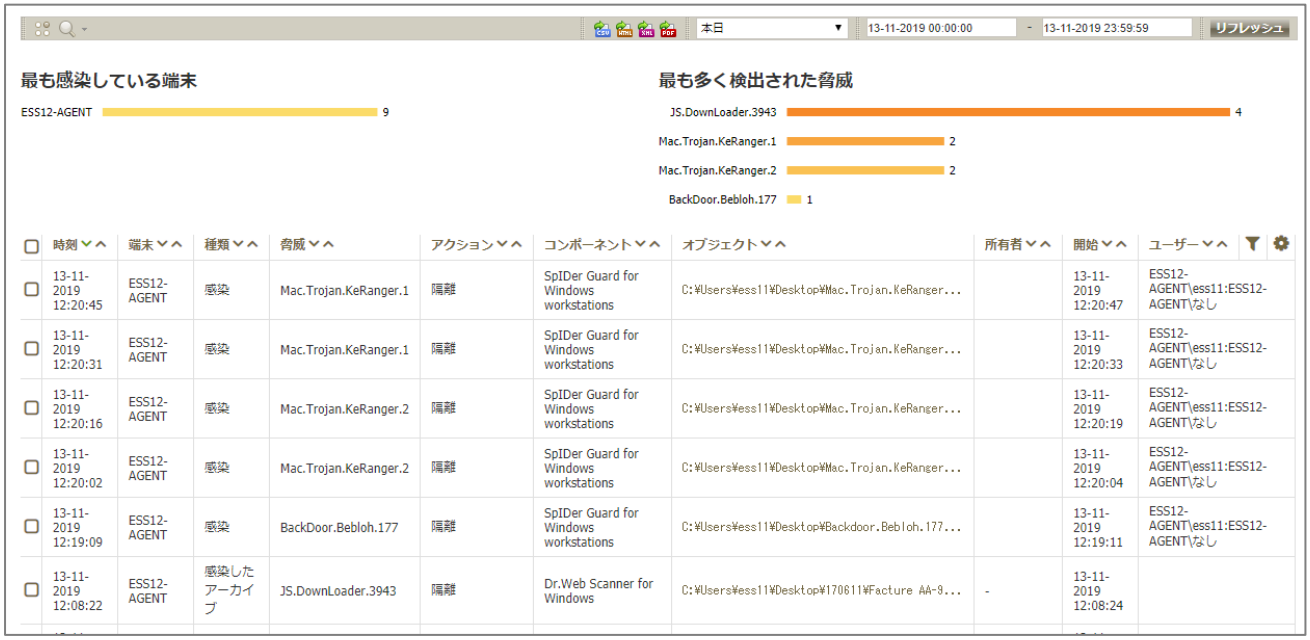
- スキャンしたファイル数　①の箇所
- 検出された脅威の数　②の箇所
- 削除された脅威の数　③の箇所
- 隔離された脅威の数　④の箇所
- ブロックされた脅威の数　⑤の箇所
- 平均スキャン速度(Byte/s)　⑥の箇所

最初に選択したグループ全体の情報が表示され、その下に端末単位での情報が表示されます。



7.12.2　脅威

「脅威」から指定した期間における、選択したグループ全体・端末毎の検出された脅威およびそのアクションの内容等を確認することができます。



時刻	端末	種類	脅威	アクション	コンポーネント	オブジェクト	所有者	開始	ユーザー
13-11-2019 12:20:45	ESS12-AGENT	感染	Mac.Trojan.KeRanger.1	隔離	SpIDer Guard for Windows workstations	C:¥Users¥ess11¥Desktop¥Mac.Trojan.KeRanger...		13-11-2019 12:20:47	ESS12-AGENT\ess11:ESS12-AGENT\なし
13-11-2019 12:20:31	ESS12-AGENT	感染	Mac.Trojan.KeRanger.1	隔離	SpIDer Guard for Windows workstations	C:¥Users¥ess11¥Desktop¥Mac.Trojan.KeRanger...		13-11-2019 12:20:33	ESS12-AGENT\ess11:ESS12-AGENT\なし
13-11-2019 12:20:16	ESS12-AGENT	感染	Mac.Trojan.KeRanger.2	隔離	SpIDer Guard for Windows workstations	C:¥Users¥ess11¥Desktop¥Mac.Trojan.KeRanger...		13-11-2019 12:20:19	ESS12-AGENT\ess11:ESS12-AGENT\なし
13-11-2019 12:20:02	ESS12-AGENT	感染	Mac.Trojan.KeRanger.2	隔離	SpIDer Guard for Windows workstations	C:¥Users¥ess11¥Desktop¥Mac.Trojan.KeRanger...		13-11-2019 12:20:04	ESS12-AGENT\ess11:ESS12-AGENT\なし
13-11-2019 12:19:09	ESS12-AGENT	感染	BackDoor.Bebloh.177	隔離	SpIDer Guard for Windows workstations	C:¥Users¥ess11¥Desktop¥Backdoor.Bebloh.177...		13-11-2019 12:19:11	ESS12-AGENT\ess11:ESS12-AGENT\なし
13-11-2019 12:08:22	ESS12-AGENT	感染したアーカイブ	JS.DownLoader.3943	隔離	Dr.Web Scanner for Windows	C:¥Users¥ess11¥Desktop¥170811¥Facture AA-9...	-	13-11-2019 12:08:24	

- コンポーネント　脅威を検出したコンポーネント名が表示されます。
- アクション　検出された脅威に対して行われた処理が表示されます。「脅威に対してアクションを自動的に適用」が有効でない場合、Dr.Web Scanner にてファイルのスキャンを実行した場合には、「レポート」が表示されます。

7.13クローズドネットワークでの定義ファイル等の更新

インターネットに接続されていないクローズドネットワーク内で利用される場合、以下の方法で定義ファイル等の更新を行なうことが可能です。

この場合も、クローズドネットワーク内に ESS サーバを用意し、クローズドネットワーク内の他の端末には ESS Agent をインストールしてください。また、定義ファイル等のダウンロードの際には、インターネットに接続可能な Windows 端末が必要となります。

7.13.1 Dr.Web Repository Loader のダウンロード

弊社ダウンロードサイトより Dr.Web Repository Loader をダウンロードします。

※ Dr.Web Repository Loader を実行する OS に対応したものをダウンロードしてください。

※ 「Windows, GUI」は、GUI 版の Dr.Web Repository Loader となります。以降は、GUI 版の Dr.Web Repository Loader での説明となります。

7.13.2　Dr.Web Repository Loader の実行

1) ダウンロードした Dr.Web Repository Loader(GUI 版)を定義ファイル等のダウンロードに用いる Windows 端末上のフォルダ(C:¥TMP 等)にコピーします。

   32bit 用　：　drweb-reploader-gui-windows-x86.exe

   64bit 用　：　drweb-reploader-gui-windows-x64.exe

2) Agent.key を Dr.Web Repository Loader をコピーした Windows 端末上の同じフォルダにコピーします。

3) Dr.Web Repository Loader を実行します。

※　Agent.key が表示されていない場合は、参照ボタンから Agent.key を指定してください。

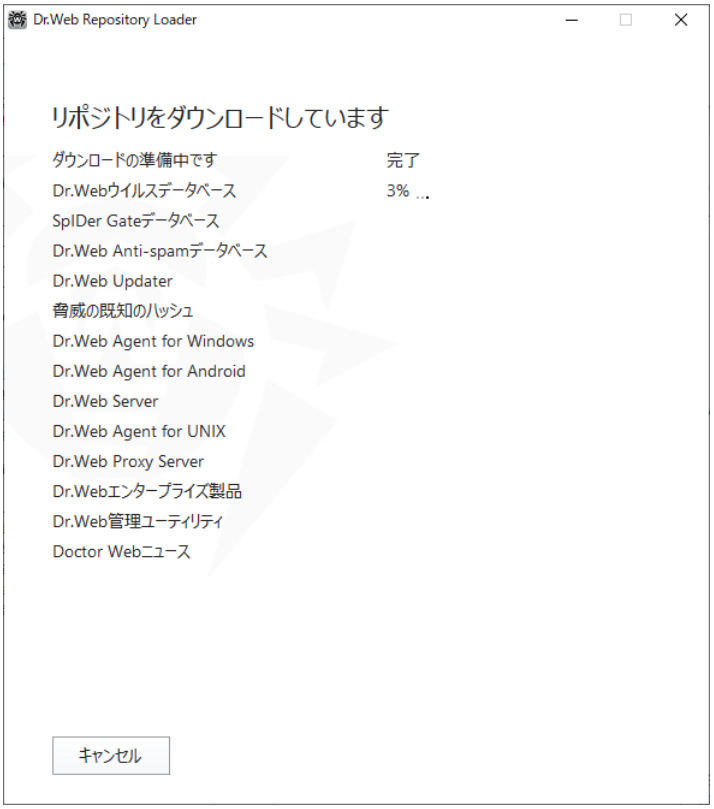
※　「ダウンロード先フォルダ」は、初期値では Dr.Web Repository Loader を実行したフォルダとなります。

※　「追加パラメータ」からプロキシの設定やダウンロード対象の指定が可能です。

※　データ量が非常に大きくなる(約 20GB 以上)ため、必要なもののみダウンロードすることを推奨します。

4) 「ダウンロード」ボタンをクリックします。

5) リポジトリのダウンロードが開始します。

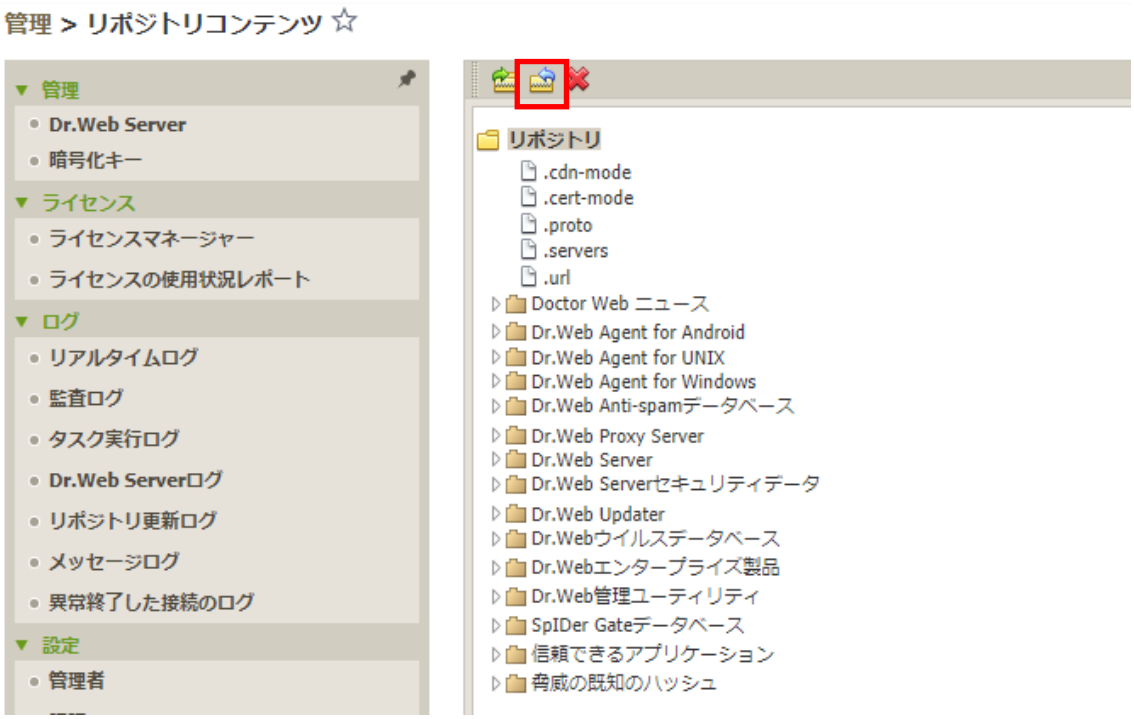


6) 下記が表示されたら「OK」ボタンをクリックし、保存された zip ファイルを USB メモリ等にコピーします。

7) クローズドネットワーク内の CC にログインします。

8) 「管理」メニューから「レポジトリコンテンツ」を開きます。

9) 「リポジトリファイルを含んだアーカイブをインポート」アイコンをクリックします。



10) 虫眼鏡のアイコンをクリックし、6)で保存した zip ファイルを指定します。

11) 「インポート」ボタンをクリックすると、リポジトリが取り込まれます。

12) 取り込みが完了した後、「管理」メニューから「リポジトリの状態」を開き、定義ファイル等が更新されたことを確認します。

7.14Dr.Web Proxy

Dr.Web Proxy を使用すると、ESS サーバと Dr.Web Agent 間の直接接続が不可能な場合(ESS サーバと Dr.Web Agent がパケットルーティングを持たない別々のネットワークにある場合等)でも、Dr.Web Agent を ESS サーバに接続させることができます。また、ESS12 では、インストール済みの Dr.Web Agent for Windows に Dr.Web Proxy を追加したり、Dr.Web Agent for Windows のインストールと同時に Dr.Web Proxy をインストールすることができます。

※ Agent のインストールと同時にインストールする場合には、「リンクされた Dr.Web Proxy Server を作成」等のオプションを指定した状態で端末(Agent)毎に専用のインストーラを作成する必要があります。

7.14.1 ESS サーバの設定変更

1) CC にログインします。
2) 「管理」メニューから「Dr.Web Server の設定」を開き、「モジュール」タブを開きます。
3) 「**Dr.Web Proxy Server プロトコル**」を**有効**にします。
4) 「ネットワーク」タブを開き、「トランスポート」を開きます。
5) 暗号化の設定を「**いいえ**」に変更します。
6) 「保存」クリックし、設定を保存します。
7) 再起動要求が表示された場合、再起動ボタンをクリックして再起動します。

7.14.2 Dr.Web Proxy のインストール

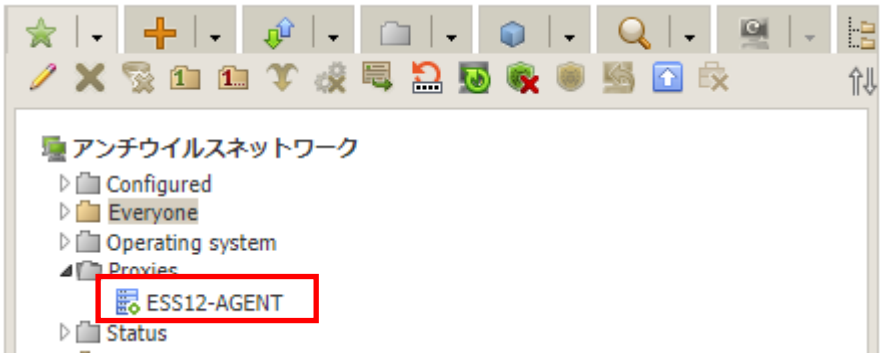
1) CC にログインします。
2) 「アンチウイルスネットワーク」メニュー中央のツリーから Dr.Web Proxy をインストールする端末を選択します。
   ※ Dr.Web Proxy をインストールする端末には固定 IP を付与してください。
3) 画面右側に表示された「端末〇〇 のプロパティ」の個所を下にスクロールし、「Dr.Web Proxy Server」セクションまで移動します。
4) 「リンクされた Dr.Web Proxy Server を作成」にチェックを入れます。

5) 必要事項を入力した後、「保存」をクリックします。

6) 「アンチウイルスネットワーク」メニュー中央のツリー内に「Proxies」グループ配下に追加したプロキシサーバーが表示されたことを確認します。

7) しばらく待ち、プロキシサーバーのアイコンの状態が水色に変わったことを確認します。

※ 以下の例では、IP アドレスの表示を有効にしています。



7.14.3 Dr.Web Proxy の設定変更

7.12.2 の操作を行うと「アンチウイルスネットワーク」メニュー中央のツリー内に「Proxies」というグループが表示されますので、共通の設定または個別の設定を行います。

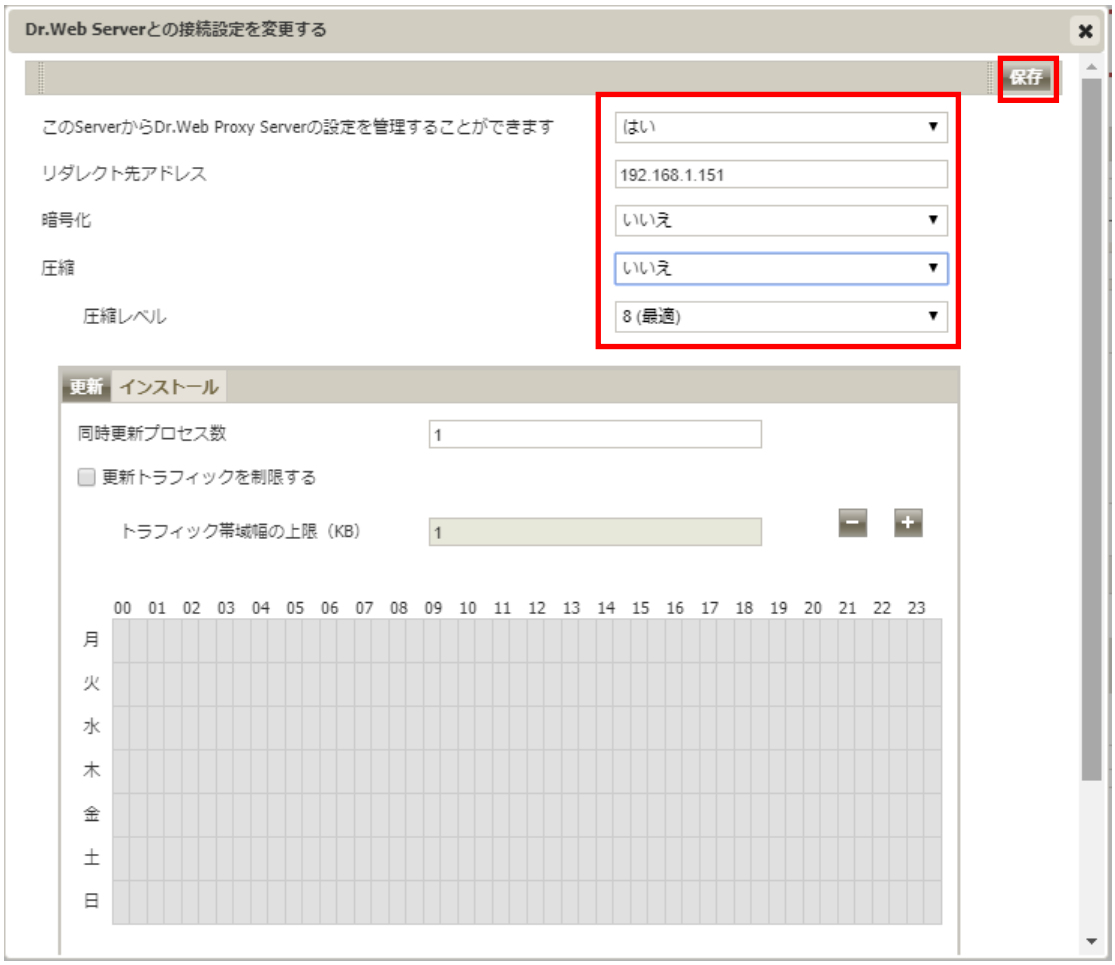
1) 「アンチウイルスネットワーク」メニュー中央のツリー内の「Proxies」グループ、またはその配下にある個別設定を行う端末(プロキシサーバー)を選択します。

2) 画面左側の「Dr.Web Proxy Server」を開きます。

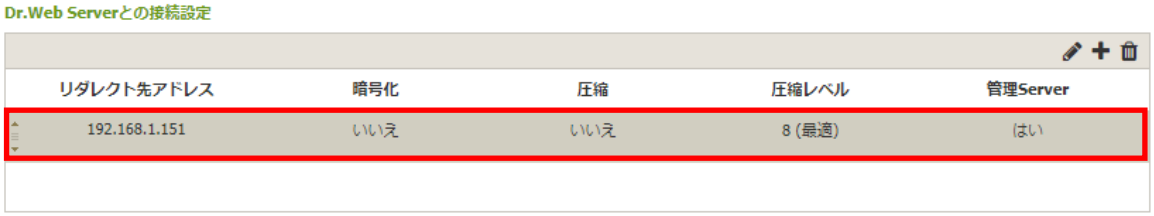
3) 「待ち受け(リッスン)」タブを開き、「Dr.Web Server との接続設定」内に表示されているものを選択し、変更ボタン(鉛筆のアイコン)をクリックします。

4) 「この Server からプロキシサーバーの設定を管理することができます」を「はい」に変更し、次の項目を設定し、「保存」をクリックします。

- リダイレクト先アドレス
  ESS サーバの IP アドレス(または DNS 名)を入力してください。
- 「暗号化」および「圧縮」
  「いいえ」または「可能であれば」に設定してください。
  ※ [Dr.Web Server の設定]-[ネットワーク]-[トランスポート]の「暗号化」および「圧縮」の設定と同じにしてください。



5) 「Dr.Web Server との接続設定」内の表示が変更されたことを確認します。



6) 「キャッシュ」タブをクリックし、「キャッシュを有効にする」にチェックを入れ、「整合性チェックモード」を「アイドル」に変更し、「プロアクティブキャッシングを有効にする」にチェックを入れます。

※ 同期が不要な項目については、チェックを外してください。

7) 「保存」をクリックして、設定を保存します。

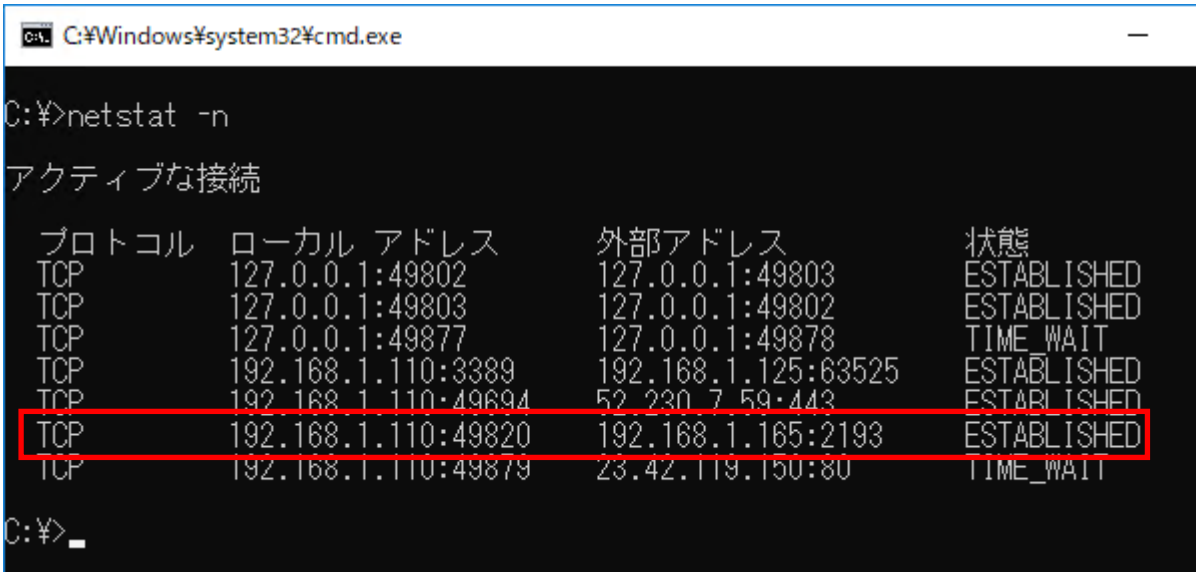
7.14.4 Dr.Web Proxy 経由での Dr.Web Agent for Windows のインストール

Dr.Web Agent for Windows を Dr.Web Proxy 経由でのインストールの際は、ESS サーバのアドレスとして Dr.Web Proxy がインストールされた端末の IP アドレスを指定して、インストールを実行してください。

7.14.5　インストール済み Dr.Web Agent for Windows の接続先変更

インストール済み Dr.Web Agent for Windows を Dr.Web Proxy 経由で ESS サーバに接続させるには、以下の操作を行なってください。

1) CC にログインします。
2) 「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対象の端末を選択します。
3) 「接続設定」を開き、「Server」欄に Dr.Web Proxy がインストールされた端末の IP アドレスと ESS サーバのアドレスを追加し、「保存」をクリックします。
   ※　Dr.Web Proxy が停止している場合に、直接 ESS サーバに接続できるよう両方登録してください。
4) しばらく待ち、CC 上で当該端末が接続されたことを確認します。
5) 当該端末上でコマンドプロンプトを開き「netstat -n」コマンドを実行し、Dr.Web Proxy がインストールされた端末と 2193 ポートの通信が行われていることを確認します。
   ※　以下は、Dr.Web Proxy がインストールされた”192.168.1.165”の端末に接続できている場合の表示です。



7.15DB の変更（IntDB → SQLite3）

ESS12 では、ESS6 では初期設定されている IntDB はサポートされていません。そのため、ESS10 サーバを IntDB で利用されている場合(ESS6 からアップグレードした場合等が該当)には、ESS12 にアップグレードする前に DB を SQLite3 に変更する必要があります。

1) ESS10 を停止します。

```
# /etc/init.d/drwcsd stop
```

※ 停止後、drwcsd のプロセスが動作していないことを確認してください。

2) “/var/opt/drwcs”フォルダ内の DB ファイルの状況を確認します。
   - database.dbs のタイムスタンプが、ESS10 を停止した日時のものである事。
   - database.sqlite と database.sqlite-journal がフォルダ内に存在していない事。
     database.sqlite のみがフォルダ内に存在している場合、ファイルをリネームしてください。

3) IntDB をファイルにエクスポートします。

```
# /etc/init.d/drwcsd exportdb /var/opt/drwcs/log/dbexport
```

4) “/var/opt/drwcs/log/drwcsd.log”を確認し、最後の行に「[Server] Exit code 0x0/0 (success)」と出力されていることを確認します。

5) drwcsd.conf を変更します。

```
# vi /var/opt/drwcs/etc/drwcsd.conf
```

6) “<IntDB”で始まる行を以下のようにコメントアウトします。

```
<!--
<intdb dbfile="database.dbs" cachesize="2048" synchronous="FULL" />
 -->
```

7) 次の行をコメントアウトした行の下に追加します。

```
<sqlite cachesize='2048' dbfile='database.sqlite' synchronous='FULL'/>
```

8) DB を初期化します。

```
# /etc/init.d/drwcsd initdb
```

9) “/var/opt/drwcs/log/drwcsd.log”を確認し、最後の行に「[Server] Exit code 0x0/0 (success)」と出力されていることを確認します。

10) “/var/opt/drwcs”フォルダ内に以下のファイルが作成されたことを確認します。

database.sqlite

database.sqlite-journal

11) DB をファイルからインポートします。

```
# /etc/init.d/drwcsd importdb /var/opt/drwcs/log/dbexport
```

12) “/var/opt/drwcs/log/drwcsd.log”を確認し、最後の行に「[Server] Exit code 0x0/0 (success)」と出力されていることを確認します。

13) ESS10 を起動します。

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

14) Control Center にログインし、既存の端末が正常に接続できているか確認します。

7.16 Dr.Web Agent for Windows のアンインストール

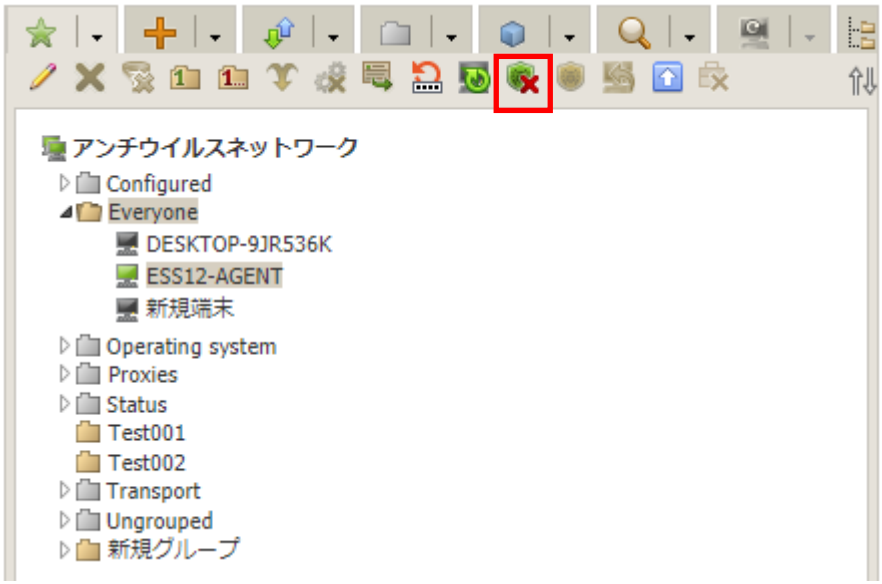
Dr.Web Agent for Windows は、次の方法でアンインストールすることができます。

- CC 上から
- クライアント PC 上から
  - CC 上で、アンインストールが許可されている必要があります。

7.16.1 CC 上からのアンインストール

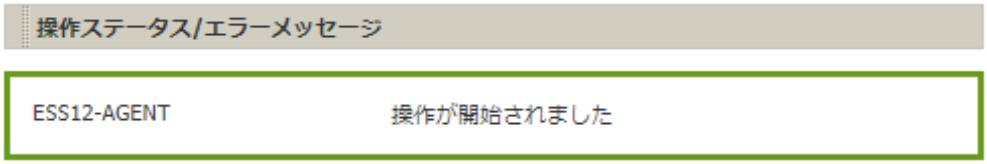
この方法でアンインストールするためには、Agent が CC に接続している必要があります。

1) CC にログインします。
2) 「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対象の端末を選択します。
3) ツリー上部の全般アイコン(星型のアイコン)をクリックし、下図の赤枠のアイコン(Dr.Web のアイコンに赤い×印がついたアイコン)をクリックします。



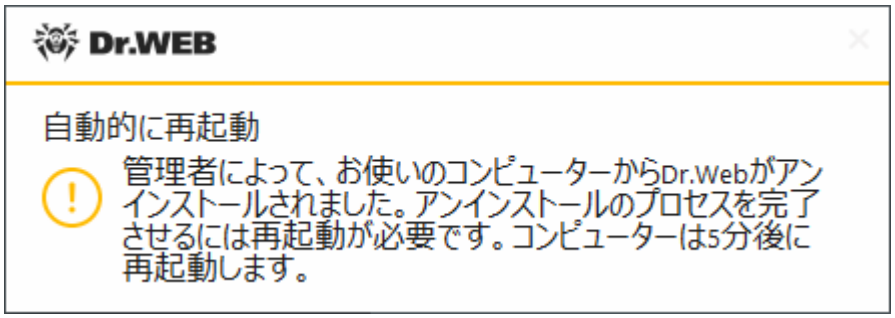
4) 以下のようなアンインストールの確認メッセージが表示されたら、「OK」をクリックします。

5) 以下のような表示がされたことを確認します。

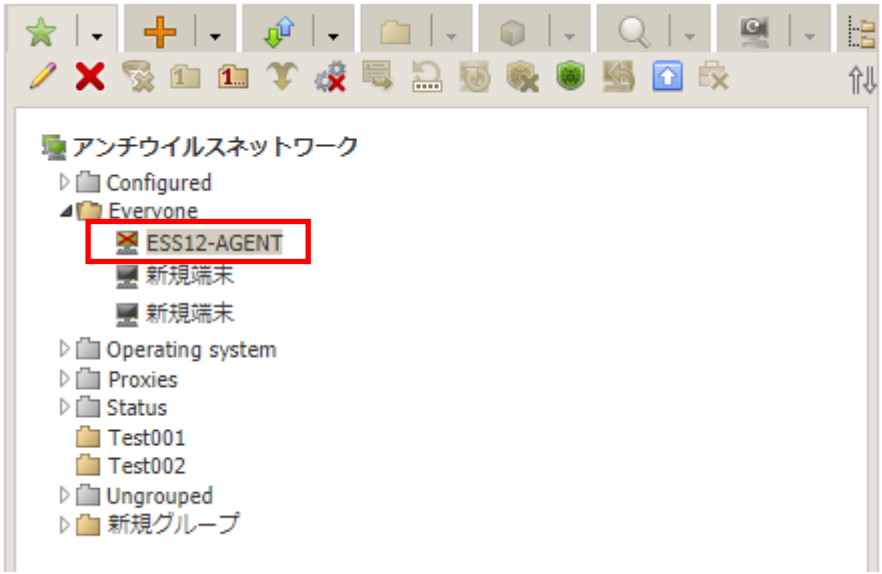


6) クライアント PC 上に以下のようなメッセージが表示されたら、PC を再起動してください。

※ 手動での再起動を実行しなくても、5 分後に自動的に再起動されます。



7) CC 上では、アンインストールされた端末には以下のように赤い×がついた状態で表示されます。



※ この状態でもライセンスを消費していますので、必要に応じて CC 上から端末を削除してください。

7.16.2 クライアント PC 上からのアンインストール

この方法でアンインストールするためには、CC 上で Dr.Web Agent のアンインストールが許可されており、その設定が Agent に連携されている必要があります。

※ CC の「アンチウイルスネットワーク」メニューで、対象の端末を選択後、「パーミッション」を開き「全般」タブの「Dr.Web Agent をアンインストールする」にチェックが入っているか、予めご確認ください。

1) コマンドプロンプトを起動します。

2) 以下のコマンドを実行します。

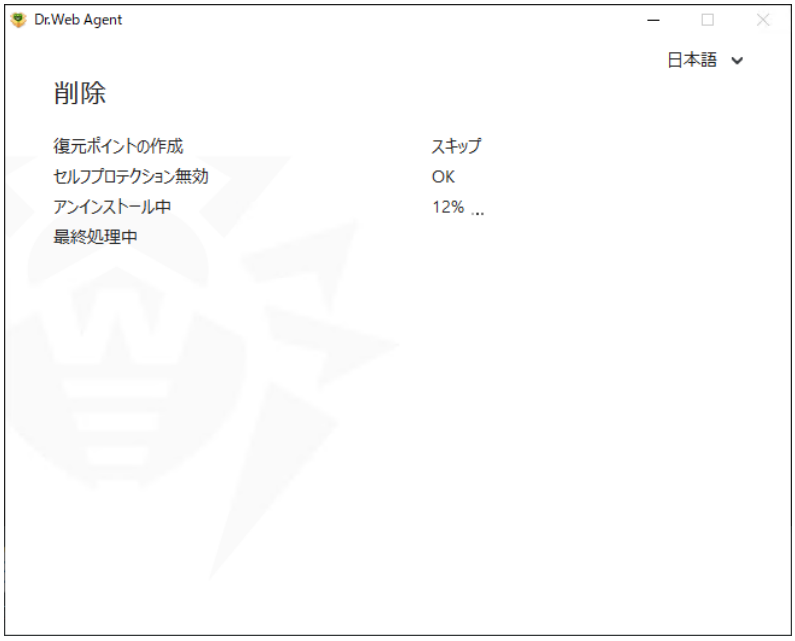
```
C:¥ > "C:¥ProgramData¥Doctor Web¥Setup¥drweb-es-agent¥win-es-agent-setup.exe" /instmode remove /silent no
```

※ 「ユーザーアカウント制御」の画面が表示されたら「はい」をクリックしてください。

3) 以下の画面で「次へ」をクリックします。

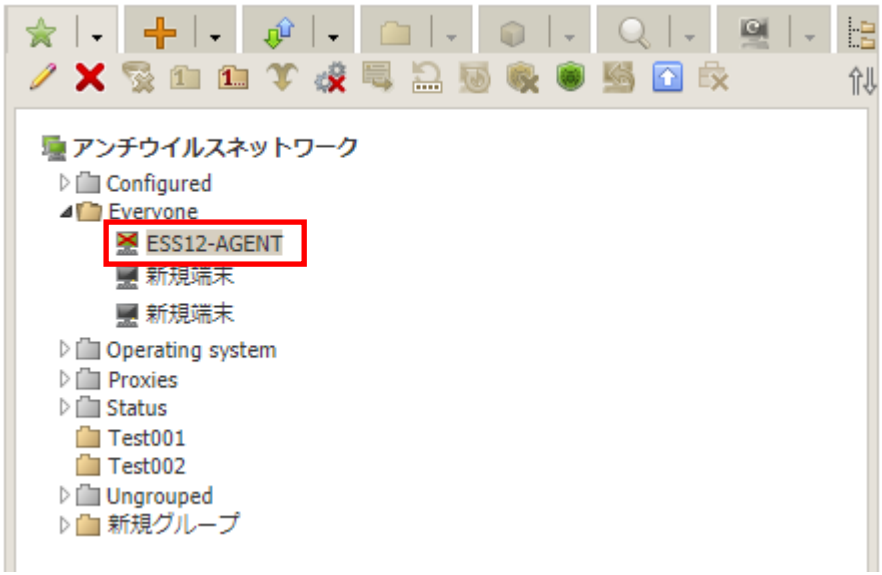
4) 以下の画面で「削除」をクリックします。

5) アンインストールが開始します。



6) 以下の画面が表示されたら、「すぐに再起動」をクリックして PC を再起動してください。

7) CC 上では、アンインストールされた端末には以下のように赤い×がついた状態で表示されます。



※ この状態でもライセンスを消費していますので、必要に応じて CC 上から端末を削除してください。

7.16.3 アンインストールに失敗する場合の対処

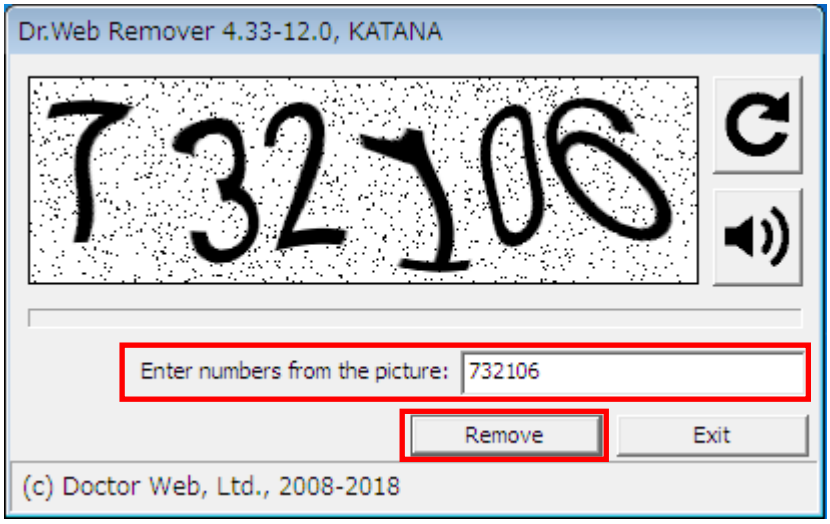
7.14.1 および 7.14.2 の手順でアンインストールができなかったり(CC と接続が不可でアンインストールが許可されていない場合等)、エラーとなる場合には、以下の URL から削除ツールをダウンロードして、ご利用ください。

https://download.geo.drweb.com/pub/drweb/tools/drw_remover.exe

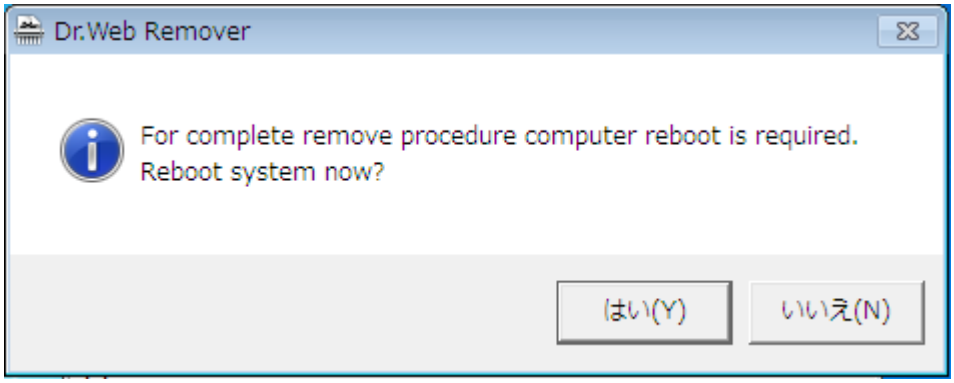
削除ツール(”drw_remover.exe”)を使用して、Dr.Web Agent をアンインストールした場合、他の方法と異なり CC 上の端末アイコンには赤い×は表示されず、オフライン端末と同じようにグレーの状態となります。

1) 上記 URL から削除ツールをダウンロードします。
   ※ ”drw_remover.exe”は、都度ダウンロードしてください。ご利用中の Dr.Web Agent に未対応の”drw_remover.exe”を使用すると、削除が適切に実行されない場合があります。
2) ダウンロードした” drw_remover.exe”を実行します。
   ※ 「ユーザーアカウント制御」の画面が表示されたら「はい」をクリックしてください。

3) 画面に表示されている数字を「Enter numbers from the picture:」の箇所に入力し、「Remove」をクリックします。



4) 以下の画面が表示されたら、「はい」をクリックして PC を再起動します。



※ 削除後もライセンスを消費していますので、必要に応じて CC 上から端末を削除してください。

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/

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