



Dr.Web Enterprise Security Suite

Ver.11 簡易構築ガイド

-Linux 用-

株式会社 Doctor Web Pacific

初版 : 2018/06/26

改訂 : 2021/10/20



目次

1.	はじめに.....	4
1.1	ライセンス証書の受領.....	4
1.2	ライセンス証書に含まれる内容.....	4
2.	環境前提条件.....	4
3.	準備.....	5
3.1	インストール環境の確認.....	5
3.2	ファイル.....	5
4.	インストール.....	6
4.1	インストーラのパーミッションの変更.....	6
4.2	インストーラの実行.....	6
4.3	キーファイルの登録と表示言語の変更.....	7
5.	Control Center の設定.....	10
5.1	ESS サーバの更新【必須】.....	10
5.2	「Dr.Web Server の設定」の変更.....	10
5.3	「Web サーバーの設定」の変更.....	11
5.4	「通知設定」の変更【推奨】.....	12
5.5	Dr.Web Agent 設定の変更.....	13
6.	Agent のインストール.....	15
6.1	Agent のインストールの前に.....	15
6.1.1	導入するコンポーネントの選択.....	15
6.1.2	その他注意事項等.....	16
6.2	Agent のインストーラの配布とインストール、承認.....	18
6.2.1	Agent のインストーラの配布.....	18
6.2.2	Agent のインストール、承認.....	18
6.3	その他の Agent のインストール方法.....	22
6.3.1	端末毎の専用インストーラ.....	22
6.3.2	Windows OS 向けエージェントインストーラフルパッケージ.....	24
7.	ケーススタディ.....	26
7.1	管理者(admin)パスワードの変更.....	26
7.2	ライセンスの更新.....	27
7.3	Agent のインストールに失敗する.....	29
7.4	端末の追加に失敗する.....	30
7.5	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.....	30



7.6	スケジュールスキャン設定時の注意事項	30
7.7	リポジトリの更新による PC の再起動を止めたい	31
7.8	PC のクローニングについて	31
7.8.1	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	31
7.8.2	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	33
7.8.3	構築済みの ESS サーバがない場合	33
7.9	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	33
7.10	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	34
7.11	統計情報	35
7.11.1	スキャン統計情報	35
7.11.2	脅威	36
7.12	クローズドネットワークでの定義ファイル等の更新	37
7.13	Dr.Web Proxy	41
7.13.1	ESS サーバの設定変更	41
7.13.2	Dr.Web Proxy のインストール	41
7.13.3	Dr.Web Proxy の設定変更	42
7.13.4	Dr.Web Proxy 経由での Dr.Web Agent for Windows のインストール	44
7.13.5	インストール済み Dr.Web Agent for Windows の接続先変更	45
7.14	Dr.Web Agent for Windows のアンインストール	46
7.14.1	CC 上からのアンインストール	46
7.14.2	クライアント PC 上からのアンインストール	47
7.14.3	アンインストールに失敗する場合の対処	50



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、弊社集中管理ツール(Enterprise Security Suite/Control Center)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。

- customer(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)

※ “My Dr.Web”につきましては、日本ではご利用できません。

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。

- CentOS 7.5 (64bit)
- FirewallD、SELinux は無効
- Enterprise Security Suite (以降、ESS)を新規インストール
- 内部 DB(SQLite3)を使用



3. 準備

3.1 インストール環境の確認

➤ 通信ポート

以下のポートの通信が可能であるか確認してください。

TCP : 2193,139,445

UDP : 2193,139,445

http : 80, 9080

https : 443, 9081

➤ モジュール

lsb : v.3 以降

glibc : v.2.7 以降

※ メモリ、HDD 容量等については、インストールマニュアルを参照してください。

3.2 ファイル

以下のファイルを用意してください。インストーラおよび Agent.key 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。

➤ インストーラ

インストール対象の Linux にあった.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。

➤ Agent.key(ライセンスキーファイル)

Agent.key を用意してください。

4. インストール

4.1 インストーラのパーミッションの変更

インストーラ(.run ファイル)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>
```

4.2 インストーラの実行

- 1) 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。

- 2) 「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。

- 3) 「To continue the installation, you must accept the License Agreement. Accept? (yes/NO)」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。

- 4) 以下の内容が表示されたら、「0」を入力し、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.  
  
:
```

※ ユーザ、グループの作成、ファイルのコピー等が始まります。

- 5) 以下のメッセージが表示された後、Control Center の admin ユーザのパスワードを確認します。

```
Generating new GOST private/public key pair ...  
Keys written to "/var/opt/drwcs/etc/drwcsd.pri" and "/var/opt/drwcs/etc/drwcsd.pub" (1  
pass, 3 ms)  
Public key /var/opt/drwcs/etc/drwcsd.pub moved to /opt/drwcs/webmin/install  
Generating self signed SSL certificate ...  
Initializing new database ...  
Making initial product revision ...  
Installation of drweb-esuite is complete.  
  
Automatically generated administrator password is 81QWOFChBD  
  
Installation completed.  
#
```

※ 上記の例では、81QWOFChBD がパスワードとなります。パスワードはランダムに生成されるため必ずメモしてください。



- 6) 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。

```
# service drwcsd status
Dr.Web Server is started
#
```

4.3 キーファイルの登録と表示言語の変更

- 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。

The image shows a login form with two input fields. The first field is labeled 'Login' and the second is labeled 'Password'. Both fields are outlined with a red border. Below the fields is a button labeled 'Log in'.

ID : admin

Password : インストールの最後に表示されたもの

※ パスワードが不明な場合には、以下の方法で確認できます。

```
# /opt/drwcs/bin/drwidbsh3 /var/opt/drwcs/database.sqlite
SQLite version 3.21.0 2017-10-24 18:55:49
Enter ".help" for usage hints.
sqlite> .headers on
sqlite> select * from admins;
id|login|password|fname|mname|lname|descr|addr|lastseenfrom|lastseenat|createtime|
modtime|externalauth|langcode|datecode
c9687f73-d21d-b211-a797-85419c46f0e6|admin|81QWOFChBD|||Default administrator
account|||0|20180621064301412|20180621064301412|0|
sqlite> .exit
#
```

admin の次のフィールドの文字列(上記の例では、赤字で示した 81QWOFChBD)がパスワードとなります。

- 3) 画面右上にある「Preferences」アイコンをクリックします。



- 4) 「Interface language」を”English”から”日本語”に変更し、「Save」ボタンをクリックします。

General

Login*	<input type="text" value="admin"/>
First name	<input type="text"/>
Middle name	<input type="text"/>
Last name	<input type="text"/>
Interface language	<input type="text" value="English"/> ▼
Date format	<input type="text" value="DD-MM-YYYY HH:MM:SS"/> ▼
Last address	<input type="text" value="https://192.168.1.125:65180:27"/>
Creation date	<input type="text" value="21-06-2018 15:43:01"/>
Modification date	<input type="text" value="21-06-2018 15:43:01"/>
Description	<input type="text" value="Default administrator account"/>

- 5) 表示が英語から日本語に変更されたことを確認します。
6) 「管理」メニューに移動します。



- 7) 画面左側の[管理]-[ライセンスマネージャー]をクリックします。



- 8) 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「ライセンスキーを追加」アイコンをクリックします。



- 9) 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。



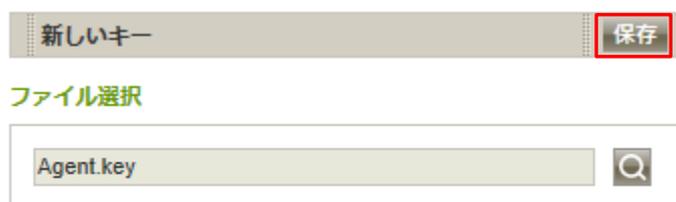
新しいキー 保存

ファイル選択

🔍

ライセンスキーをEveryoneグループに割り当てる

- 10) 予め用意してある Agent.key を指定し、「開く」をクリックします。
11) 「ライセンスキーを Everyone グループに割り当てる」にチェックを入れ、「保存」ボタンをクリックします。



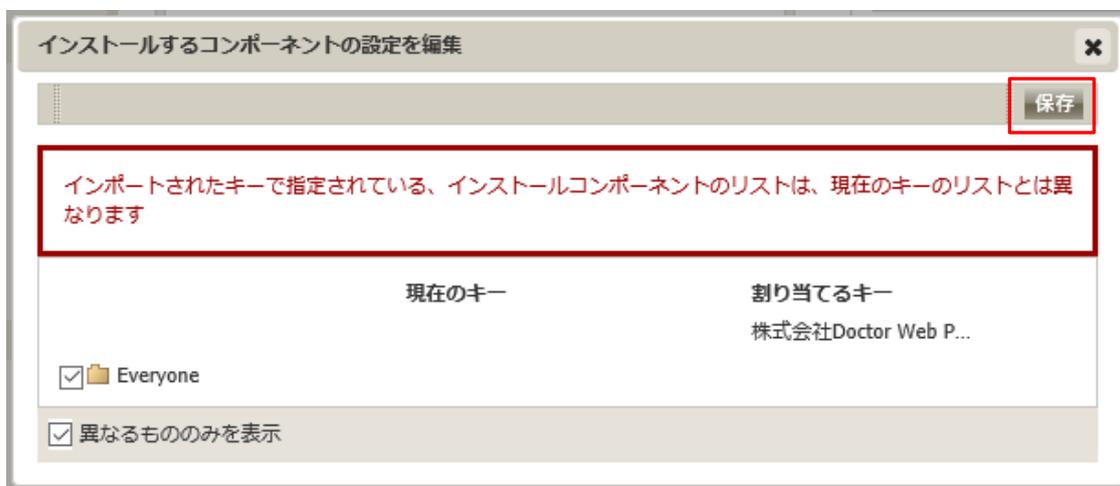
新しいキー 保存

ファイル選択

Agent.key 🔍

ライセンスキーをEveryoneグループに割り当てる

- 12) 以下のような画面が表示された場合は、「保存」ボタンをクリックします。



インストールするコンポーネントの設定を編集 ✕

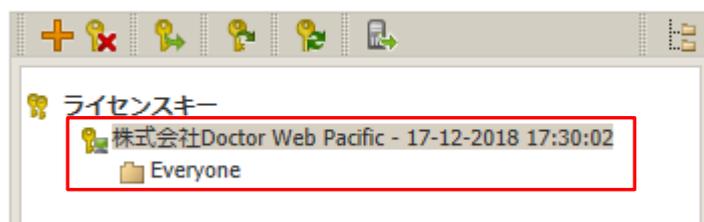
保存

インポートされたキーで指定されている、インストールコンポーネントのリストは、現在のキーのリストとは異なります

現在のキー	割り当てるキー
<input checked="" type="checkbox"/> Everyone	株式会社Doctor Web P...

異なるもののみを表示

- 13) 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が表示され、その下に「Everyone」が表示されたことを確認します。



ライセンスキー

- 株式会社Doctor Web Pacific - 17-12-2018 17:30:02
- Everyone



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いません。

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いません。

- 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 : 情報

※ ESS10 の場合、Linux 版では”トレース 3”、Windows 版では”情報”が設定されています。

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」

※ 他に「指定した時間でローテーション」が選択可能です。

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内容行われ、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。

端末

- スキャン中のエラー
- スキャン統計情報
- セキュリティに対する脅威が検出されました
- デバイスがブロックされました
- 更新を適用するには端末の再起動が必要です
- 接続が異常終了しました
- 端末アカウントを作成できません
- 端末の再起動が必要です
- 端末の認証に失敗しました
- 端末は管理者によって承認されました
- 端末は既にログインされています
- 端末は自動的に承認されました
- 端末は長い間Serverに接続されていません
- 端末更新のクリティカルエラー
- 未知の端末



5.5 Dr.Web Agent 設定の変更

5.5.1 Dr.Web Agent の言語設定 **【必須】**

初期状態では、「English」が設定されており、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ます。OS の言語と同じもので表示されるように変更します。

- 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。

5.5.2 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。

- 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。

5.5.3 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



5.5.4 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 のインストール

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導入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]から導入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。

Everyone. カスタム設定が指定されました

Dr.Web Agent for Windows	インストール必須
Dr.Web Scanner	インストール必須
Dr.Web Scanner for Windows	インストール可能
SpIDer Guard for Windows workstations	インストール可能
SpIDer Guard for Windows servers	インストール可能
SpIDer Mail for Windows	インストール可能
SpIDer Gate for Windows workstations	インストール可能
Dr.Web Office Control	インストール可能
Dr.Web for Microsoft Outlook	インストール可能
Dr.Web Anti-spam	インストール可能
Dr.Web Firewall	インストール可能

※ “SpIDer Guard for Windows workstations”と”SpIDer Guard for Windows Servers”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[レポジトリ一般設定]-[Dr.Web Agent for Windows]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、[ツール]-[サポート]-[詳細]から「プログラムについて」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

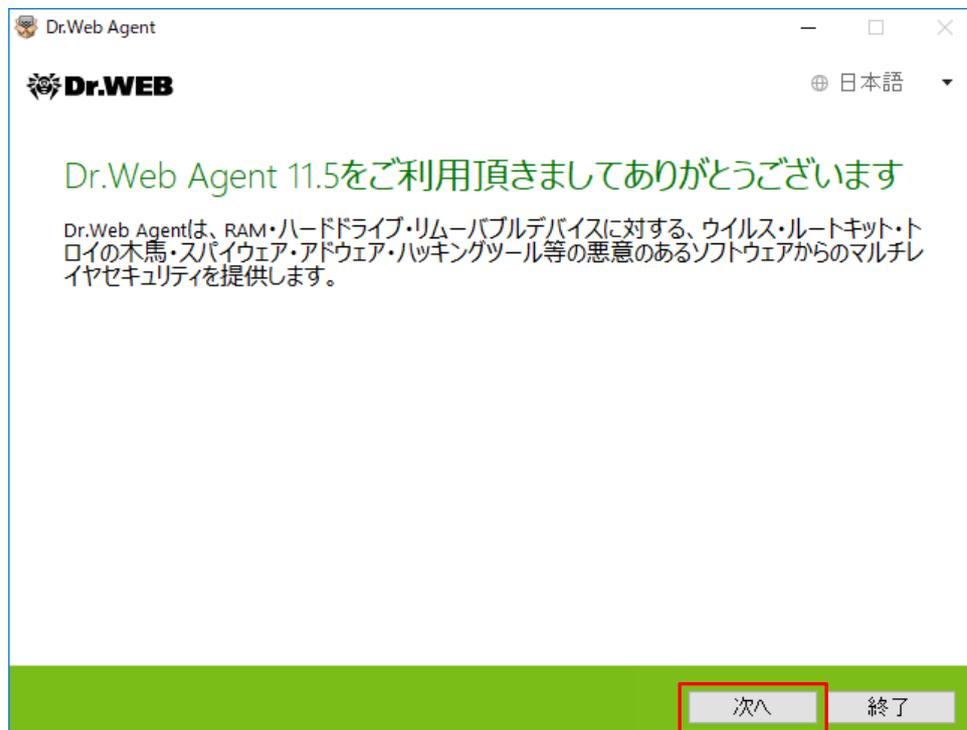
➤ 証明書

URL : <https://<ESS サーバの IP アドレス or DNS 名>:9081/install/>
<http://<ESS サーバの IP アドレス or DNS 名>:9080/install/>

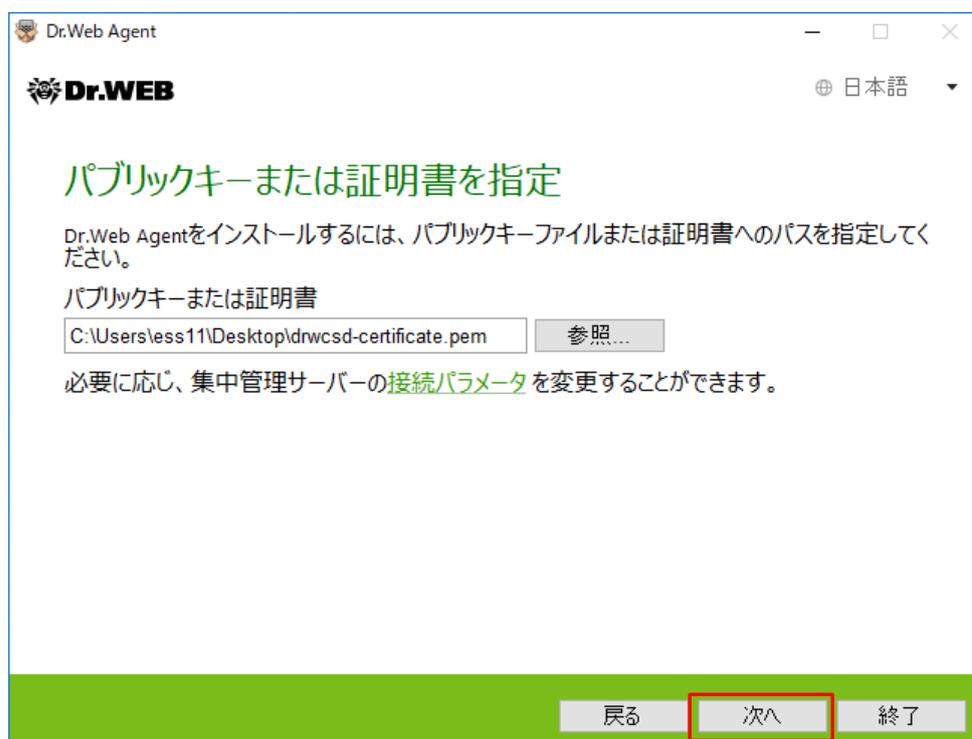
ファイル名 : drwcsd-certificate.pem

6.2.2 Agent のインストール、承認

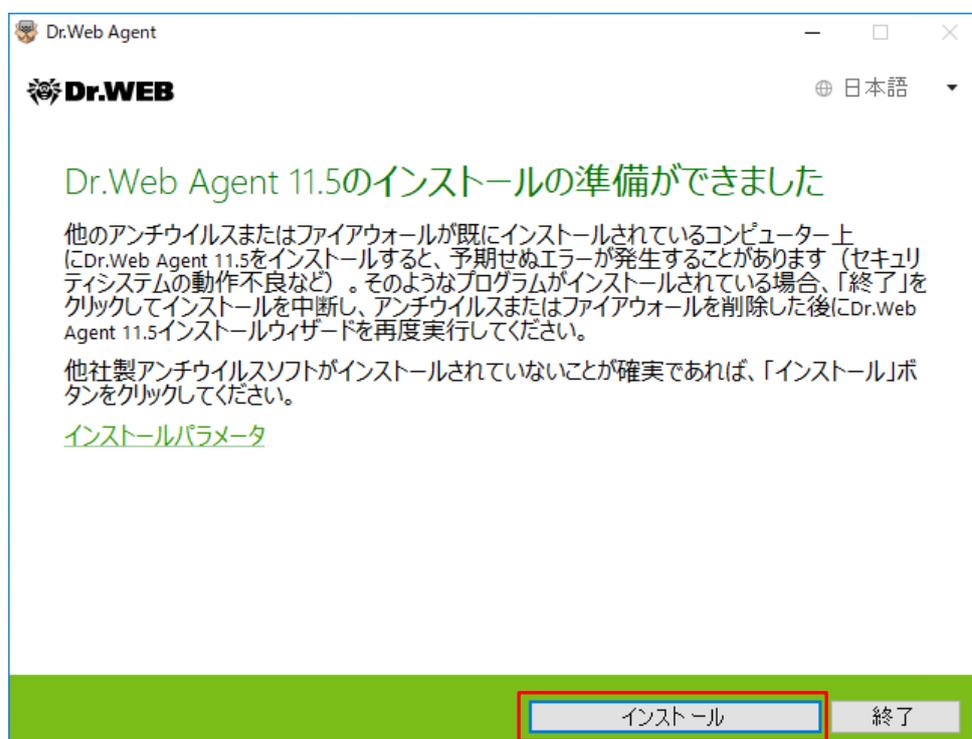
- 1) 端末上に保存した Agent のインストーラ(drwinst.exe)を実行します。
- 2) 以下の画面が表示されたら、「次へ」をクリックします。



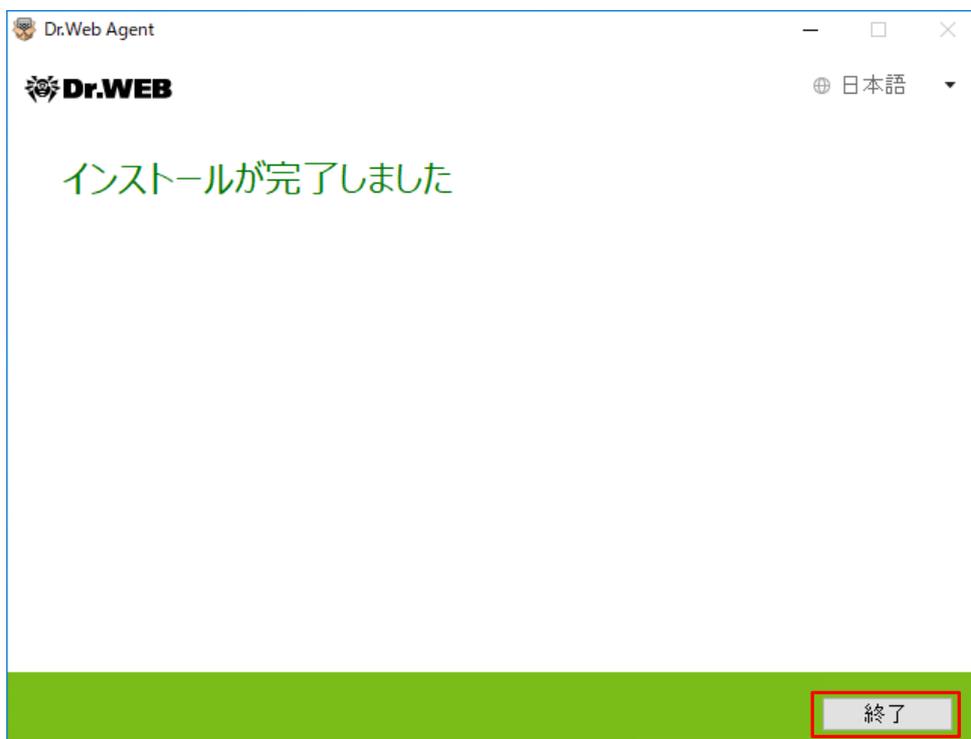
- 3) 以下の画面で暗号化キーが指定されていることを確認して、「次へ」をクリックします。



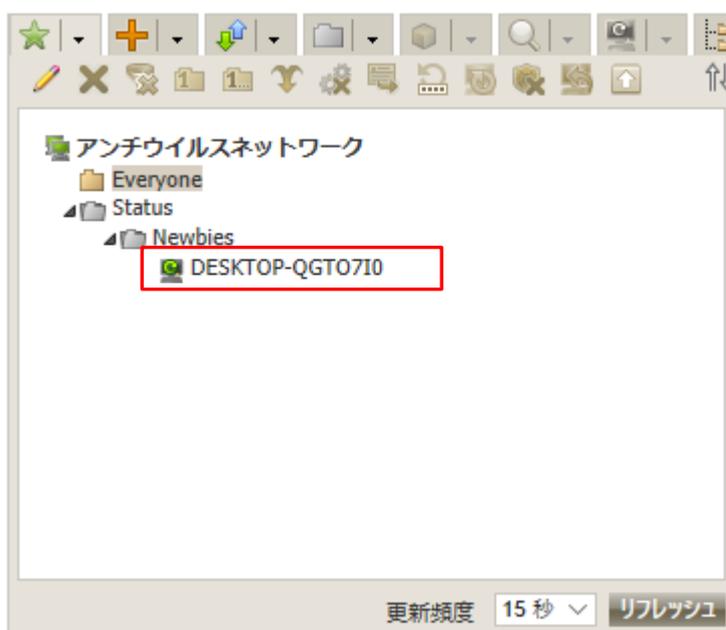
- 4) しばらくすると、以下の画面が表示されるので、「インストール」をクリックします。



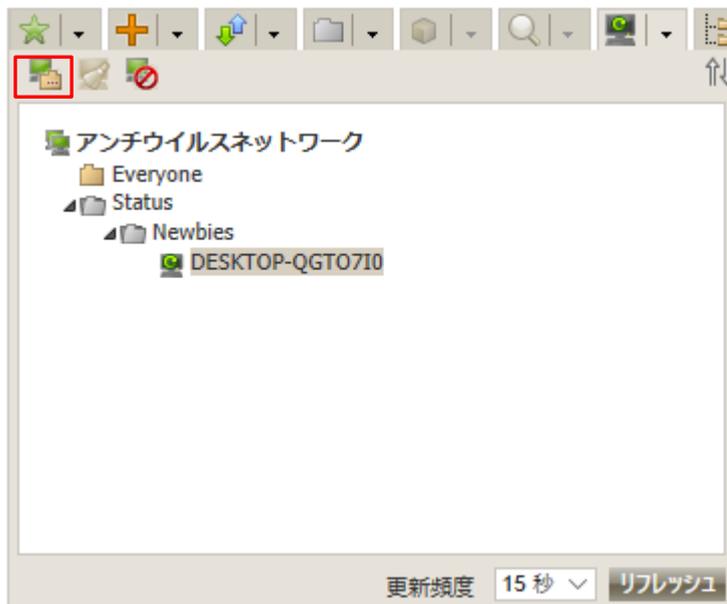
- 5) 以下の画面が表示されたら、「終了」をクリックします。



- 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。



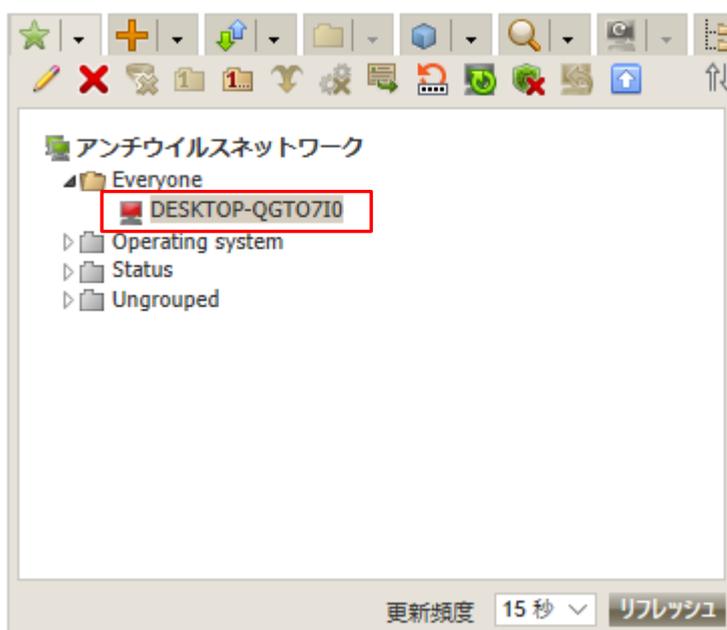
- 8) インストールした端末(以下の図では、DESKTOP-QGTO7I0)を選択し、「選択した端末を承認し、プライマリグループを設定」ボタンをクリックします。



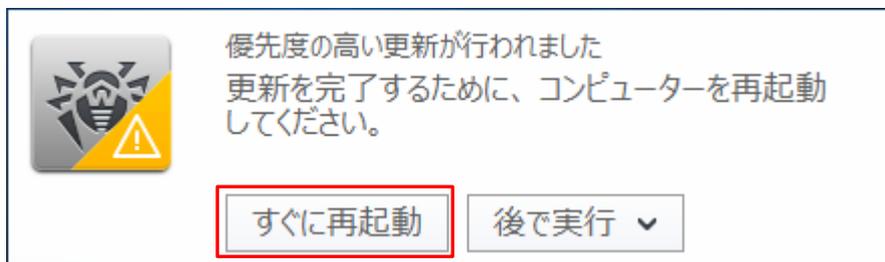
- 9) 画面右側から「プライマリグループ」を選択し、「保存」ボタンをクリックします。



- 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、「すぐに再起動」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、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 Directory 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、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。

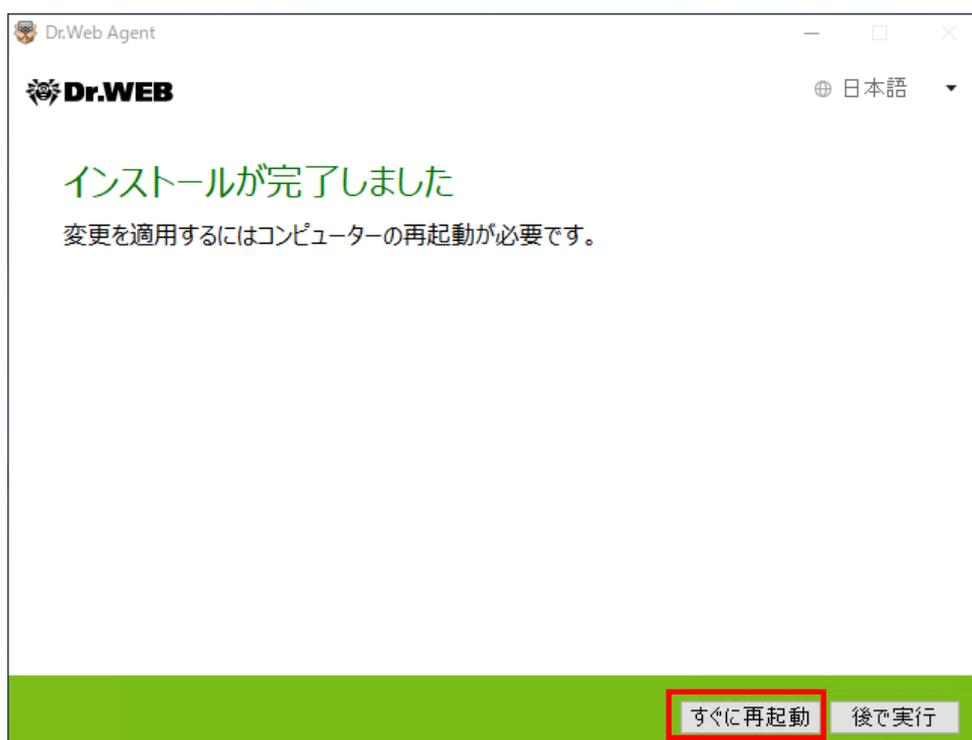


6) ダウンロードした専用インストーラ(drweb_ess_windows_<名前>.exe)をインストール対象に PC にコピーした後、実行します。

※ 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) 以下の画面が表示されたら、PC の再起動を実施します。



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

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。

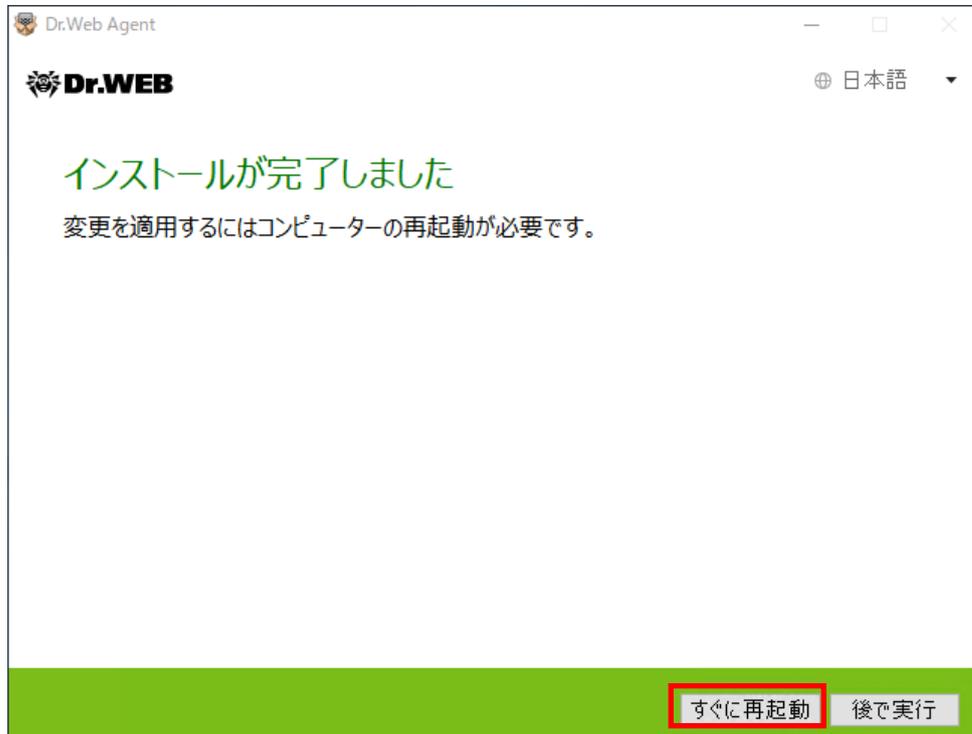


※ 2018/06/25 時点では、Ver10 用の Windows OS 向けエージェントインストーラーフルパッケージもダウンロード可能なため、バージョンに注意してください。

- 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) 以下の画面が表示されたら、PC の再起動を実施します。



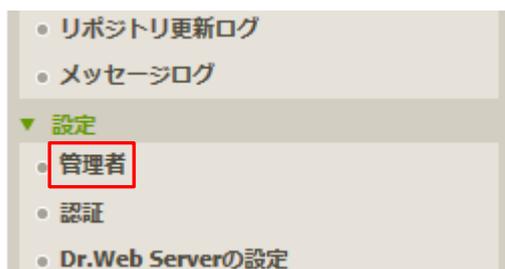
- 4) PC の再起動中に 6-1-2 の 6)~10) の手順を実行します。

※ 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。

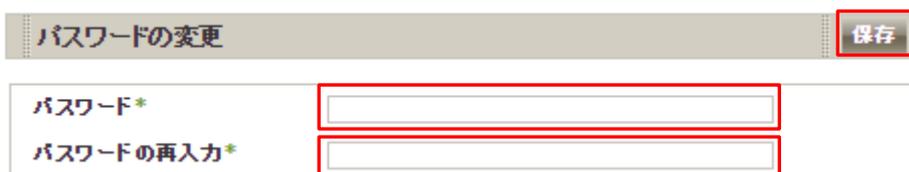


- 5) 「admin」を選択し、「パスワードの変更」アイコンをクリックします。



※ 「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。



A screenshot of a web interface showing the 'パスワードの変更' (Change Password) form. The form has a title bar with 'パスワードの変更' and a '保存' (Save) button. Below the title bar are two input fields: 'パスワード*' and 'パスワードの再入力*'. Both input fields are highlighted with red boxes.

- 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。

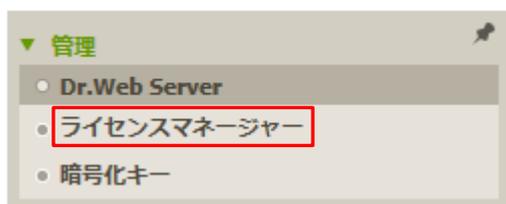
7.2 ライセンスの更新

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。

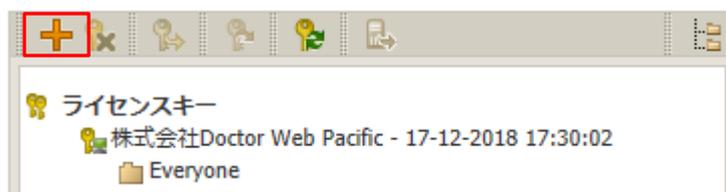
- ※ ESS11 では、ESS10 と同様に一つのグループに複数のライセンスキーを紐づけたり、逆に一つのライセンスキーに複数のグループを紐づけたりすることが可能です。ライセンスキーとグループは、1対1ではなく、n対nの関係となります。
- ※ 複数のライセンスがある場合、Everyone グループに割り当てたライセンス以外を特定のグループに紐づけることも可能です。ライセンスが紐づけられたグループをプライマリグループとして設定されている端末に、配信されます。

- 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。

管理 ☆



- 4) 画面中央の「キー」と書かれたツリーの上にある「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。



Everyoneグループのライセンスキーを置き換える

- 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。



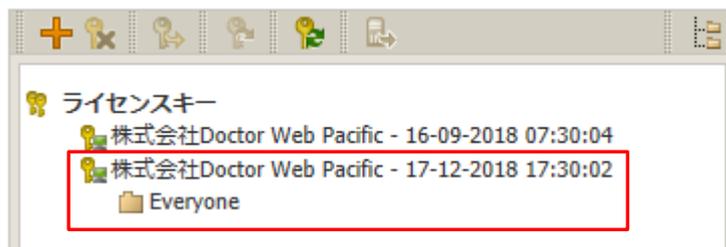
- 8) 以下のような画面が表示され、新旧のライセンスで使用可能なコンポーネントに差異が無いことを確認し、「保存」をクリックします。



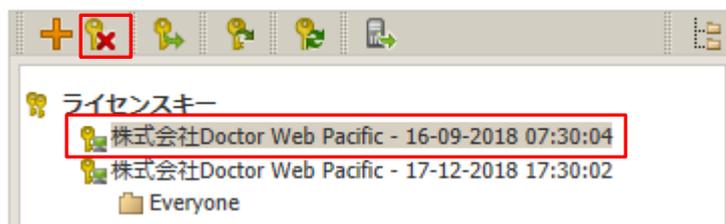
- ※ 以下のような表示は、現在のライセンスと新しいライセンスで利用可能なコンポーネントが異なることを表しています。



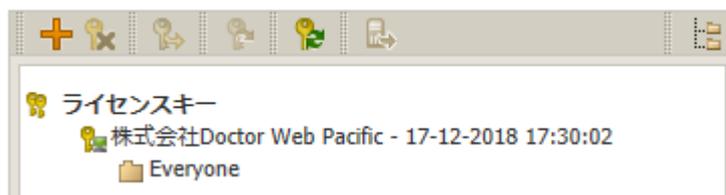
- 9) 画面中央の「キー」ツリーに追加したライセンスの「登録名」と「ライセンス終了日」が表示されたこと、「Everyone」グループが紐づいたことを確認します。



- 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。



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 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

7.5 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

7.6 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、Scanner 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。

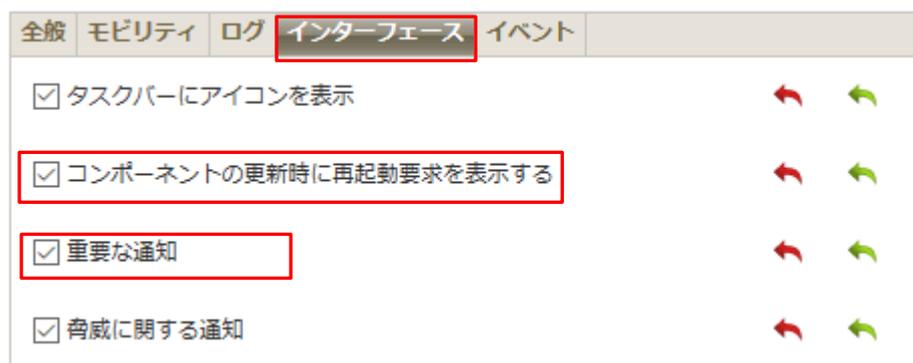
そのため、スケジュールスキャンを設定される際は、**カスタムスキャンを選択**し、手動で除外設定を行ってください。

7.7 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。

7.8 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。

7.8.1 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。



7.8.1.1. 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。

7.8.1.2. Windows OS 向けエージェントインストーラ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-11.05.0-201805220-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-11.05.0-201805220-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。

7.8.2 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。

7.8.3 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。

7.9 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。



7.10 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

7.11 統計情報

7.11.1 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。

端末	コンポーネント	①	②	③	④	⑤	⑥
ESS10-PC (c01d2083-d21d-b211-8bb6-980570842746)	SpIDer Guard for Windows workstations	359	2	0	0	0	3588914.92
DESKTOP-QGTO7I0 (7be63e22-edee-45b0-b6c5-ec68372e3c41)	SpIDer Mail for Windows	0	0	0	0	0	0
DESKTOP-QGTO7I0 (7be63e22-edee-45b0-b6c5-ec68372e3c41)	SpIDer Gate for Windows workstations	93	0	0	0	0	0
DESKTOP-QGTO7I0 (7be63e22-edee-45b0-b6c5-ec68372e3c41)	SpIDer Guard for Windows workstations	3178	4	0	0	4	3995210.98

1 ページ: 1 1~4/ 4を表示中 10



7.11.2 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。

最も感染している端末		最も多く検出された脅威	
DESKTOP-QGTO710(7be63e22-edee-45b0-b6c5-ec68372e3c41)	4	Trojan.DownLoader.26.24730	2
ESS10-PC(c01d2083-d21d-b211-8bb6-980570842746)	2	Trojan.DownLoader.26.26566	2
		Trojan.Encoder.11687	1
		W97M.DownLoader.1751	1

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	端末開始日時	ユーザー
25-06-2018 14:17:43	ESS10-PC(c01d2083-d21d-b211-8bb6-980570842746)	感染	Trojan.DownLoader.26.24730	隔離	SpiDer Guard for Windows workstations	C:\users\ess10\desktop\invoice 80675380\j3...		25-06-2018 14:16:53	ess10-PC\ess10-ess10-PC\None
25-06-2018 14:17:43	ESS10-PC(c01d2083-d21d-b211-8bb6-980570842746)	感染	Trojan.DownLoader.26.24730	隔離	SpiDer Guard for Windows workstations	C:\users\ess10\desktop\bill 81779751\b-4223...		25-06-2018 14:16:44	ess10-PC\ess10-ess10-PC\None
25-06-2018 13:05:52	DESKTOP-QGTO710(7be63e22-edee-45b0-b6c5-ec...)	感染	Trojan.DownLoader.26.26566	隔離	SpiDer Guard for Windows workstations	C:\users\ess11\desktop\ccp673641\p55633599...		25-06-2018 13:05:52	DESKTOP-QGTO710\ess11:DESKTOP-QGTO710\なし
25-06-2018 13:05:23	DESKTOP-QGTO710(7be63e22-edee-45b0-b6c5-ec...)	感染	Trojan.DownLoader.26.26566	隔離	SpiDer Guard for Windows workstations	C:\users\ess11\desktop\l49420601\p56760901...		25-06-2018 13:05:23	DESKTOP-QGTO710\ess11:DESKTOP-QGTO710\なし
25-06-2018 13:04:48	DESKTOP-QGTO710(7be63e22-edee-45b0-b6c5-ec...)	感染したコンテナ	W97M.DownLoader.1751	隔離	SpiDer Guard for Windows workstations	C:\users\ess11\desktop\36-9225.pdf		25-06-2018 13:04:58	DESKTOP-QGTO710\ess11:DESKTOP-QGTO710\なし
25-06-2018 13:04:18	DESKTOP-QGTO710(7be63e22-edee-45b0-b6c5-ec...)	感染	Trojan.Encoder.11687	隔離, 修復不可	SpiDer Guard for Windows workstations	C:\users\ess11\desktop\00-3653.pdf		25-06-2018 13:04:28	DESKTOP-QGTO710\ess11:DESKTOP-QGTO710\なし

- 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、「報告済」が表示されます。

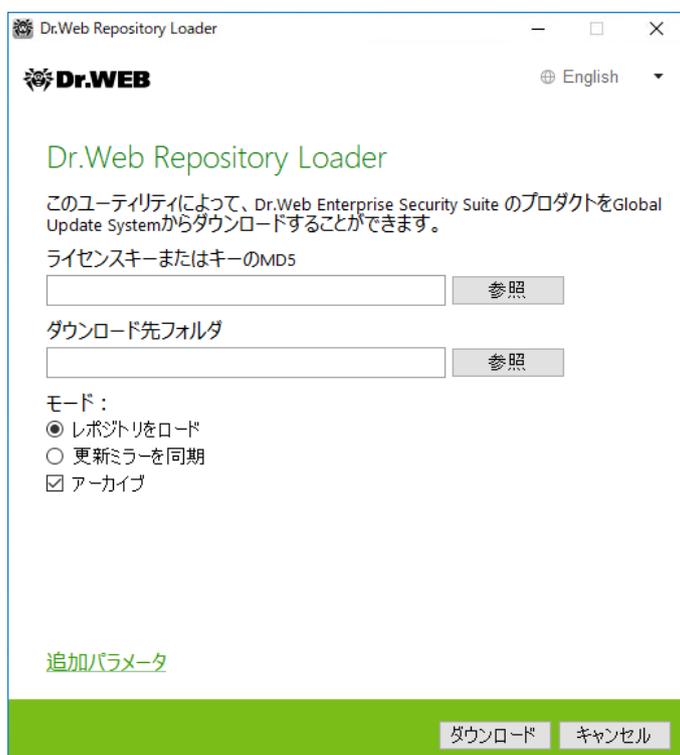


7.12 クローズドネットワークでの定義ファイル等の更新

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。

- 1) クローズドネットワーク内の CC にログインします。
- 2) 「管理」メニューから「ユーティリティ」を開きます。
- 3) 「Dr.Web Repository Loader」の個所のプルダウンから「Windows UI」を選択し、Dr.Web Repository Loader を実行する端末の OS の Bit 数にあったものを選択した後、「読み込み」をクリックします。
※ 「Windows」を選択すると、GUI 版ではなくコマンドライン版がダウンロードされます。
- 4) ダウンロードした Dr.Web Repository Loader を定義ファイル等のダウンロードに用いる Windows 端末にコピーします。
32bit 用 : drweb-reploader-gui-windows-x86.exe
64bit 用 : drweb-reploader-gui-windows-x64.exe
- 5) ダウンロードした Dr.Web Repository Loader と Agent.key を定義ファイル等のダウンロードに用いる Windows 端末にコピーします。
- 6) コピーした Dr.Web Repository Loader を実行します。



- 7) Agent.key ファイルとダウンロード先フォルダを指定した後、「ダウンロード」ボタンをクリックします。

※ 「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。

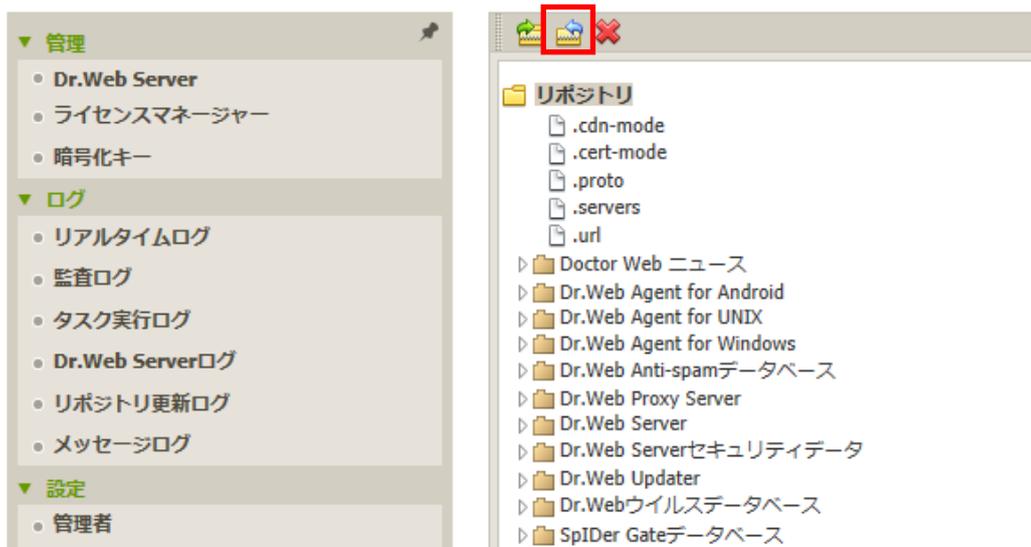
- 8) リポジトリのダウンロードが開始します。

- 9) 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。



- 10) クローズドネットワーク内の CC にログインします。
11) 「管理」メニューから「レポジトリコンテンツ」を開きます。
12) 「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。

管理 > リポジトリコンテンツ ☆





13) 虫眼鏡のアイコンをクリックし、9)で保存した zip ファイルを指定します。



14) 「読み込み」ボタンをクリックすると、リポジトリが取り込まれます。



15) 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。

管理 > リポジトリの状態 ☆

製品	現在のバージョン	最終更新日時	ステータス
Doctor Web ニュース	23-06-2018 03:10:42	23-06-2018 03:10:42	製品は正常な状態です
Dr.Web Agent for Android	25-06-2018 07:01:32	25-06-2018 07:01:32	製品は正常な状態です
Dr.Web Agent for UNIX	25-06-2018 07:11:05	25-06-2018 07:11:05	製品は正常な状態です
Dr.Web Agent for Windows	07-06-2018 11:50:41	07-06-2018 11:50:41	製品は正常な状態です
Dr.Web Anti-spamデータベース	25-06-2018 02:40:22	25-06-2018 02:40:22	製品は正常な状態です
Dr.Web Proxy Server	31-05-2018 00:00:00	31-05-2018 00:00:00	製品は正常な状態です
Dr.Web Server	31-05-2018 00:00:00	31-05-2018 00:00:00	製品は正常な状態です
Dr.Web Serverセキュリティデータ	31-05-2018 00:00:00	31-05-2018 00:00:00	製品は正常な状態です
Dr.Web Updater	31-05-2018 00:00:00	31-05-2018 00:00:00	製品は正常な状態です
Dr.Webウイルスデータベース	25-06-2018 06:07:30	25-06-2018 06:07:30	製品は正常な状態です
SpIDer Gateデータベース	25-06-2018 07:10:20	25-06-2018 07:10:20	製品は正常な状態です



7.13 Dr.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、ESS11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、「リンクされたプロキシサーバーを作成」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。

7.13.1 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サーバープロトコル」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」をクリックし、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。

7.13.2 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、「プロキシサーバー」セクションまで移動します。
- 4) 「リンクされたプロキシサーバーを作成」にチェックを入れます。

プロキシサーバー

リンクされたプロキシサーバーを作成

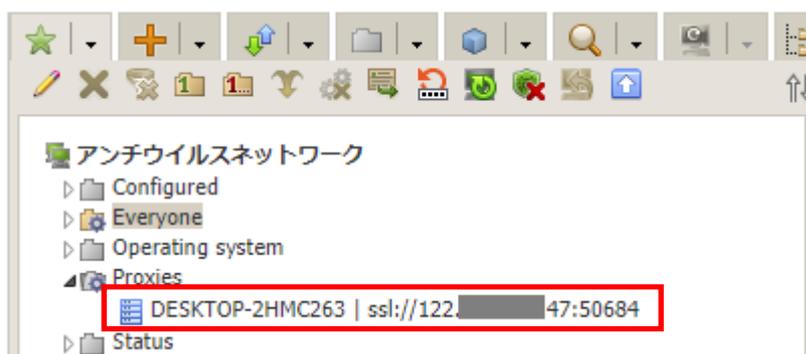
- 5) 必要事項を入力した後、「保存」をクリックします。

プロキシサーバー



Form for creating a proxy server. It includes a checked checkbox for 'Link created proxy server', an ID field with the value '1a6fd799-b640-49eb-9000-3094d20f8b53', a name field with '新しいプロキシサーバー', and empty fields for password and password confirmation. A 'Memberships' section shows a checked box for 'Proxies'.

- 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。



7.13.3 Dr.Web Proxy の設定変更

7.13.2 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。

Dr.Web Serverとの接続設定



- 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」にチェックを入れ、次の項目を設定し、「保存」をクリックします。

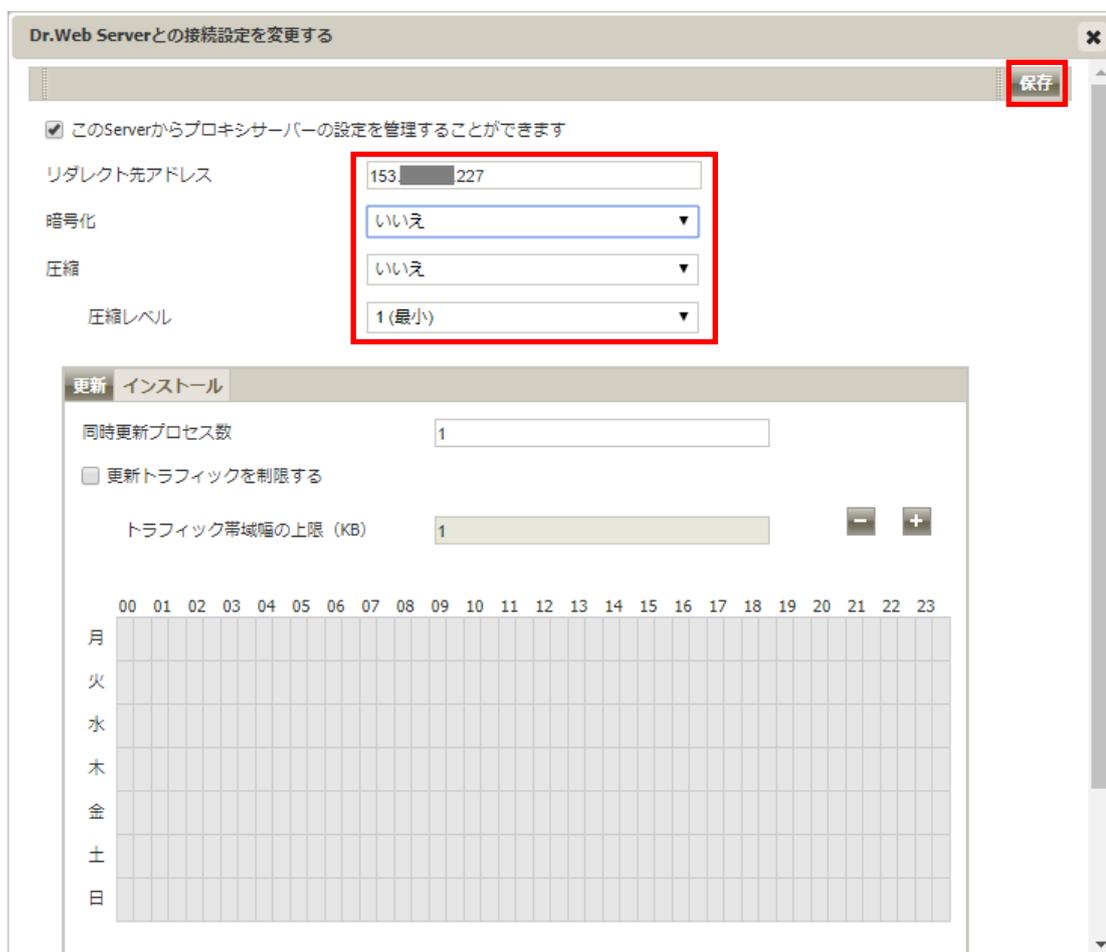
➤ リダイレクト先アドレス

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。

Dr.Web Serverとの接続設定

リダイレクト先アドレス	暗号化	圧縮	圧縮レベル	管理Server
153.███227	いいえ	いいえ	1 (最小)	✓

- 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、「同期を有効にする」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。

Proxies. カスタム設定が指定されました

証明書	待ち受け (リッスン)	キャッシュ	イベント	ダンプ	DNS
<input checked="" type="checkbox"/> キャッシュを有効にする					
リビジョンの削除間隔 (分)	60				
残るリビジョンの数	3				
使われていないファイルをアンロードする間隔 (分)	10				
整合性チェックモード	アイドル				
<input checked="" type="checkbox"/> 同期を有効にする					
<input checked="" type="checkbox"/> Dr.Web Agent for Windows					
<input checked="" type="checkbox"/> Dr.Web Agent for UNIX					
<input checked="" type="checkbox"/> Dr.Web Agent for Android					
<input type="checkbox"/> Dr.Web Server					
<input checked="" type="checkbox"/> Dr.Web Proxy Server					
<input checked="" type="checkbox"/> Dr.Web Updater					
<input checked="" type="checkbox"/> Dr.Webウイルスデータベース					
<input checked="" type="checkbox"/> SpIDer Gateデータベース					
<input checked="" type="checkbox"/> Dr.Web Anti-spamデータベース					
<input type="checkbox"/> Doctor Web ニュース					

- 7) 「保存」をクリックして、設定を保存します。

7.13.4 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。



7.13.5 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。

```
C:\Windows\system32\cmd.exe

C:\>netstat -n

アクティブな接続

プロトコル   ローカル アドレス     外部アドレス     状態
TCP         127.0.0.1:49802  127.0.0.1:49803  ESTABLISHED
TCP         127.0.0.1:49803  127.0.0.1:49802  ESTABLISHED
TCP         127.0.0.1:49877  127.0.0.1:49878  TIME_WAIT
TCP         192.168.1.110:3389  192.168.1.125:63525  ESTABLISHED
TCP         192.168.1.110:49694  52.230.7.59:443  ESTABLISHED
TCP         192.168.1.110:49820  192.168.1.165:2193  ESTABLISHED
TCP         192.168.1.110:49879  23.42.119.150:80  TIME_WAIT

C:\>
```

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

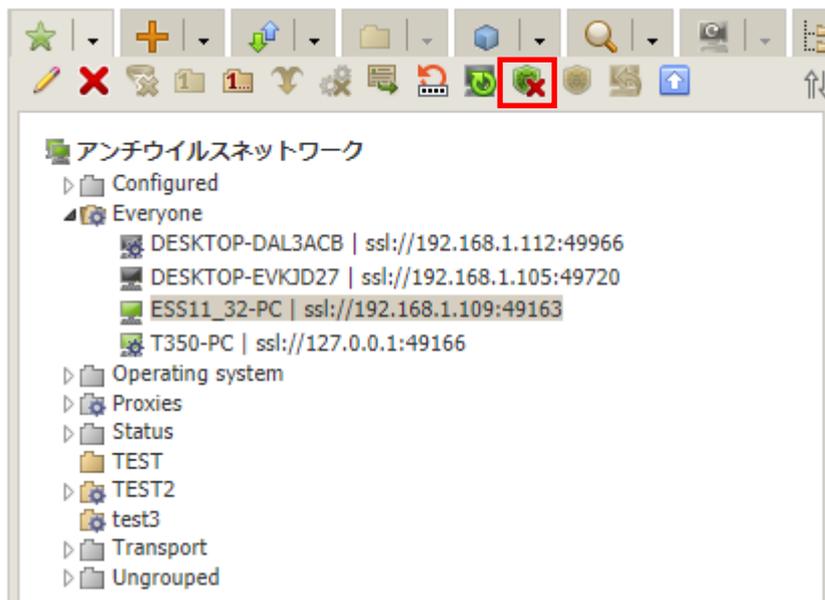
Dr.Web Agent for Windows は、次の方法でアンインストールすることができます。

- 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。

7.14.1 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。

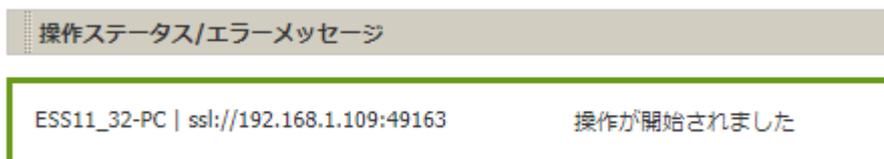
- 1) CC にログインします。
- 2) 「アンチウイルスネットワーク」メニュー中央のツリーから対象の端末を選択します。
- 3) ツリー上部の全般アイコン(星型のアイコン)をクリックし、下図の赤枠のアイコン(Dr.Web のアイコンに赤い×印がついたアイコン)をクリックします。



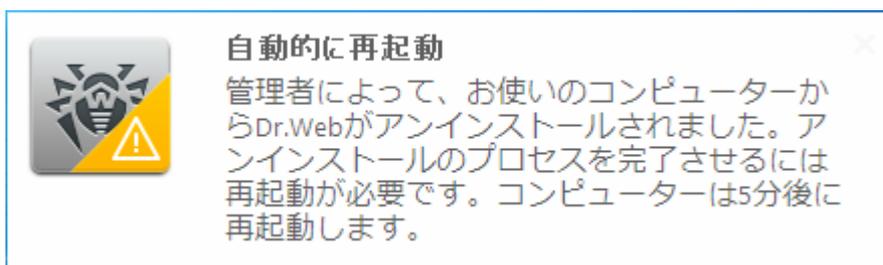
- 4) 以下のようなアンインストールの確認メッセージが表示されたら、「OK」をクリックします。



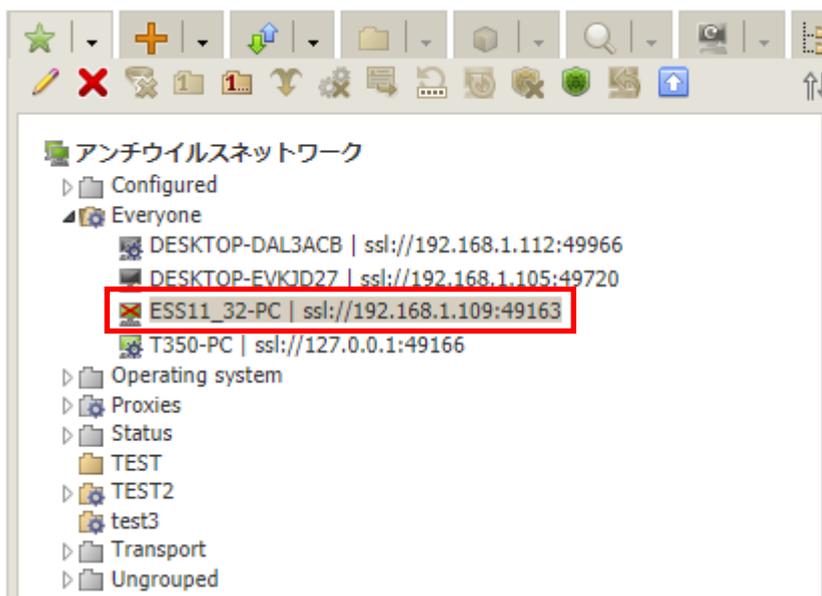
- 5) 以下のような表示がされたことを確認します。



- 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。

7.14.2 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。

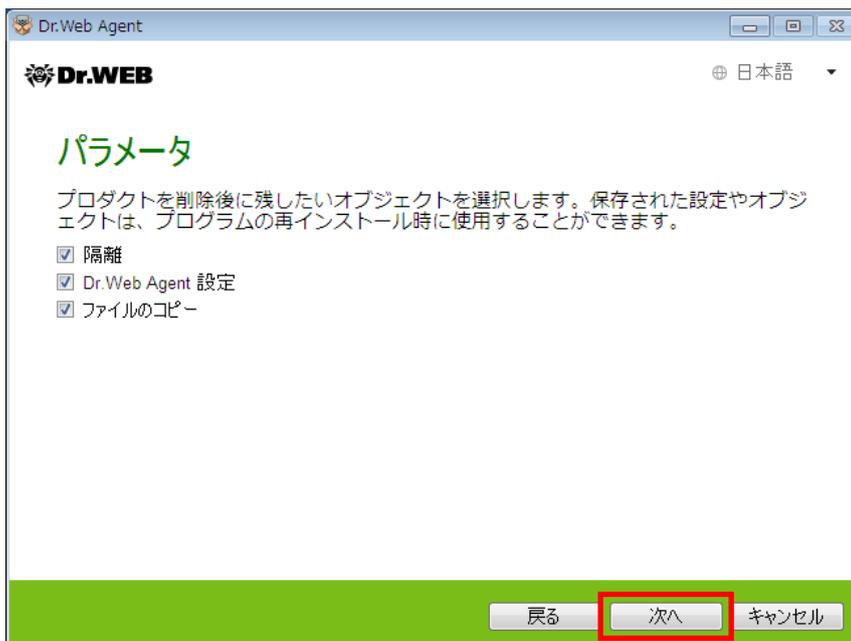
- ※ CC の「アンチウイルスネットワーク」メニューで、対象の端末を選択後、「パーミッション」を開き「全般」タブの「Dr.Web Agent をアンインストールする」にチェックが入っているか、予めご確認ください。

- 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。

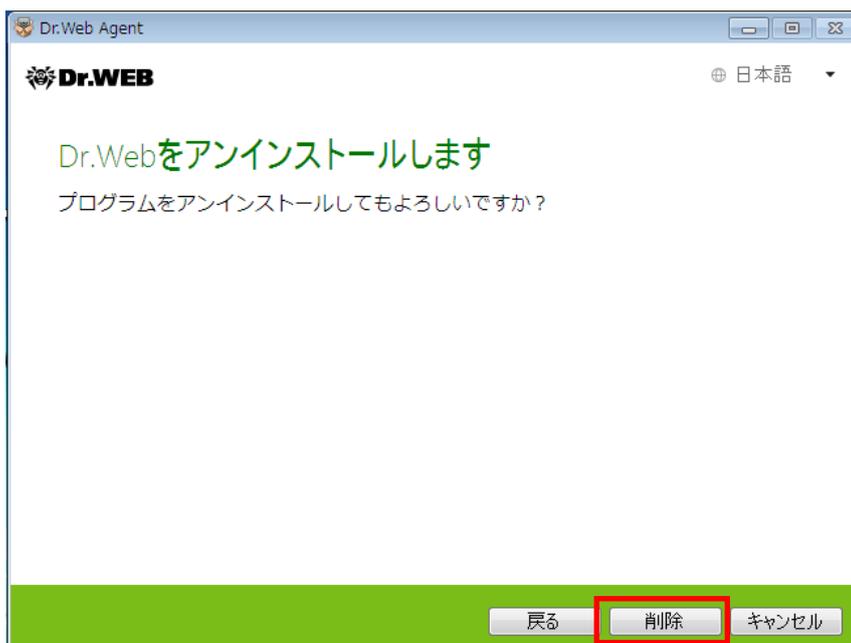
```
C:\> "C:\ProgramData\Doctor Web\Setup\win-es-agent-setup.exe" /instmode remove /silent no
```

※ 「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。

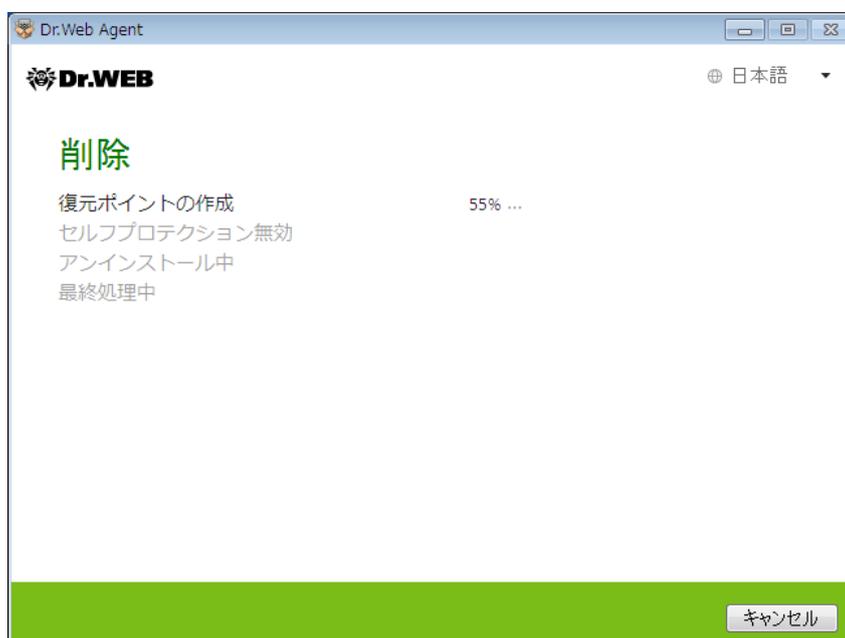


- 4) 以下の画面で「削除」をクリックします。

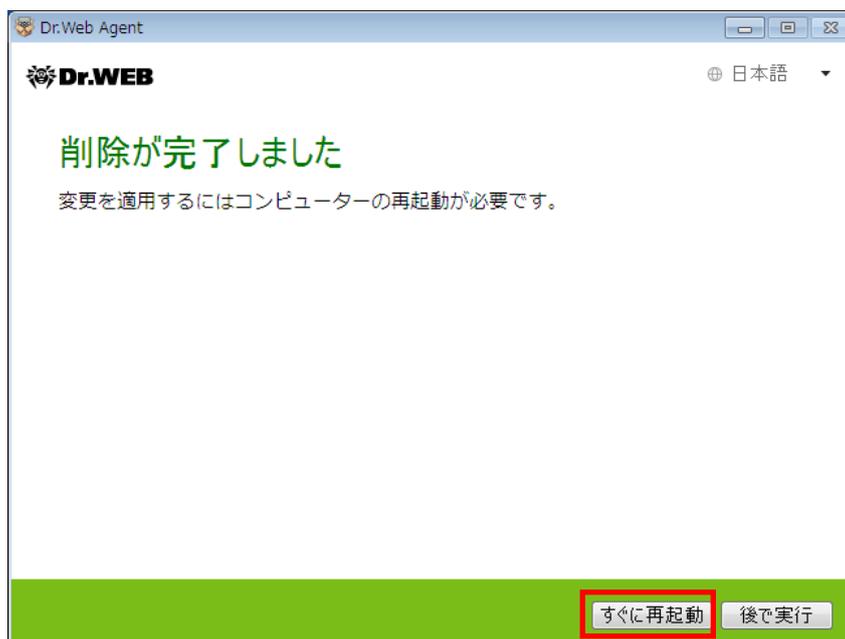




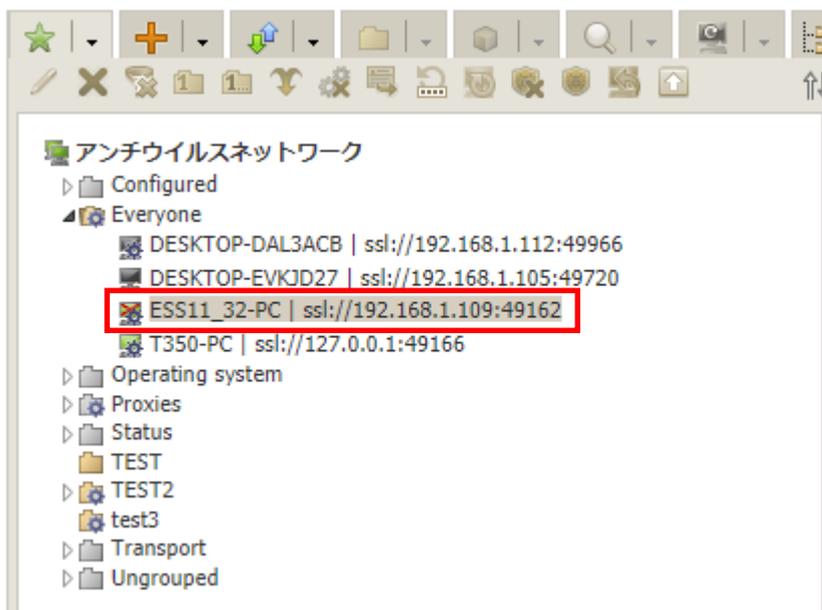
- 5) アンインストールが開始します。



- 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。

7.14.3 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 の手順でのアンインストール実施時にエラー等発生した場合には、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 のアンインストールを実施する場合、予め **Self-Protection を無効**にする必要があります。

※ Self-Protection が有効な状態では、本ツールを用いてアンインストールはできません。
また、本ツールを使用した場合には、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。

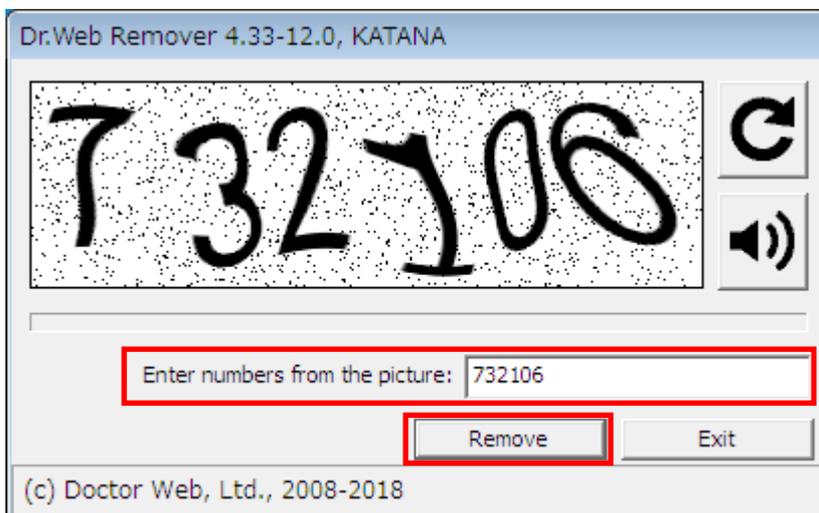
※ ”drw_remover.exe”は、都度ダウンロードしてください。ご利用中の Dr.Web Agent に未対応の”drw_remover.exe”を使用すると、削除が適切に実行されない場合があります。

2) 端末上で Self-Protection を無効にします。

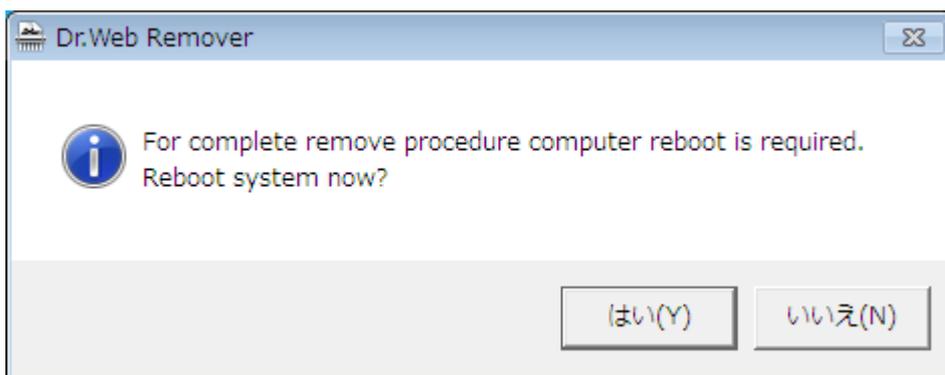
3) ダウンロードした” drw_remover.exe”を実行します。

※ 「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。

- 4) 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。



- 5) 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/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