



Dr.Web Enterprise Security Suite Ver.12 簡易構築ガイド -Linux 用-

株式会社 Doctor Web Pacific

初版 : 2019/11/15

改訂 : 2025/03/26



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.....	11
5.1	ESS サーバの更新【必須】.....	11
5.2	「Dr.Web Server の設定」の変更.....	11
5.2.1	サーバーアドレスの設定【必須】.....	11
5.2.2	暗号化設定(サーバー側)の変更【推奨】.....	12
5.2.3	Server 言語の変更【必須】.....	12
5.2.4	Server のログ設定の変更.....	12
5.3	「Web サーバーの設定」の変更.....	13
5.3.1	サーバーアドレスの変更【必須】.....	13
5.3.2	https へのリダイレクトの停止設定.....	13
5.4	「通知設定」の変更【推奨】.....	14
5.5	Dr.Web Agent 設定の変更.....	15
5.5.1	パーミッション設定の変更【推奨】.....	15
5.5.2	Dr.Web for MS Outlook の設定変更【必須】.....	15
5.5.3	hosts の除外設定【推奨】.....	16
5.5.4	Windows8、Windows10 使用時の設定変更【推奨】.....	16
5.6	Dr.Web インストールパッケージの追加.....	17
5.7	Dr.Web 管理ユーティリティの追加【推奨】.....	18
6.	Agent のインストール.....	19
6.1	Agent のインストールの前に.....	19
6.1.1	導入するコンポーネントの選択.....	19
6.1.2	その他(注意事項等).....	20
6.2	Agent のインストーラの配布とインストール、承認.....	22



6.2.1	Agent のインストーラの配布	22
6.2.2	Agent のインストール、承認.....	22
6.3	その他の Agent のインストール方法.....	26
6.3.1	端末毎の専用インストーラ.....	26
6.3.2	グループ毎の専用インストーラ	28
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	30
7.	ケーススタディ	31
7.1	管理者(admin)パスワードの変更	31
7.2	ライセンスの更新.....	32
7.3	Dr.Web Agent for Windows のインストールに失敗する	35
7.4	Dr.Web Agent for Windows の言語の変更	35
7.5	端末の追加に失敗する	35
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.....	36
7.7	スケジュールスキャン設定時の注意事項	36
7.8	リポジトリの更新による PC の再起動を止めたい.....	36
7.9	PC のクローニングについて.....	38
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	38
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.....	39
7.9.3	構築済みの ESS サーバがない場合.....	39
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.....	40
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.....	41
7.12	統計情報.....	42
7.12.1	スキャン統計情報.....	42
7.12.2	脅威.....	43
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	44
7.13.1	Dr.Web Repository Loader のダウンロード	44
7.13.2	Dr.Web Repository Loader の実行	45
7.14	Dr.Web Proxy	49
7.14.1	ESS サーバの設定変更	49
7.14.2	Dr.Web Proxy のインストール	49
7.14.3	Dr.Web Proxy の設定変更.....	50
7.14.4	Dr.Web Proxy 経由での Dr.Web Agent for Windows のインストール.....	52
7.14.5	インストール済み Dr.Web Agent for Windows の接続先変更	53
7.15	Dr.Web Agent for Windows のアンインストール.....	54
7.15.1	CC 上からのアンインストール.....	54
7.15.2	クライアント PC 上からのアンインストール	55
7.15.3	アンインストールに失敗する場合の対処.....	58



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。

- 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)

※ “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。

- Cent OS 7.7 (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

glibc : v.2.13 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。

```
Making initial product revision ...  
Installation of drweb-esuite is complete.  
  
Automatically generated password for the default administrator (admin): 7DRh9GbGeA  
  
Installation completed.  
#
```

※ 上記の例では、赤字で示した"7DRh9GbGeA"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 3.29.0 2019-07-10 17:32:03
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 | 7DRh9GbGeA | | | Default | administrator
account | https://192.168.1.125:55263:5 | | 20191112090303909 | 20191112085958743 | 20191112
085958743 | 0 | en |
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"7DRh9GbGeA")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。



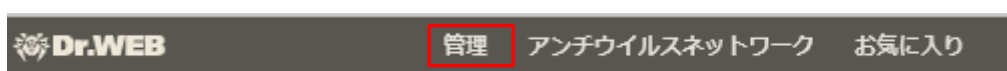
- 4) 「Interface language」を”English”から”日本語”に変更し、「Save」ボタンをクリックします。

General

Login*	admin
First name	
Middle name	
Last name	
Interface language	English ▼
Date format	DD-MM-YYYY HH:MM:SS ▼
Last address	https://192.168.1.125:55263:5
Creation date	12-11-2019 17:59:58
Modification date	12-11-2019 17:59:58
Description	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。



- 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。

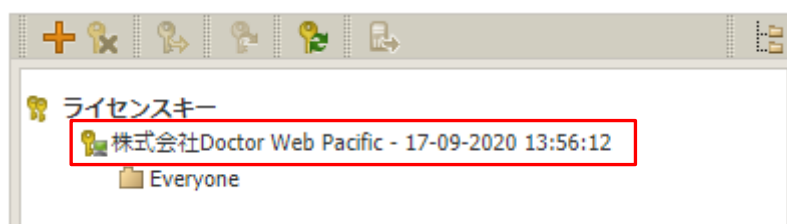


- 12) 以下のような画面が表示されるので、必要に応じて設定を変更し「保存」ボタンをクリックします。



※ 上記は包括的保護(コンプリヘンシブプロテクション)のライセンスを登録した際の画面です。

- 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。





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。

【重要】リポジトリの更新完了後、「リポジトリの更新ログ」を開いた際、「更新エリアの証明書が無効か、または信頼できません」と表示されている場合には、以下の設定を行なった後、再度上記の 1) から実行してください。

- 1) 「リポジトリの一般設定」を開きます。
- 2) 「Dr.Web GUS」タブの「更新受信」プロトコルを、「HTTP」に変更し、「保存」をクリックします。

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
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

※ 「Server ログローテーションモード」で「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の間隔を指定(初期値は 10 時間)できます。

- 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 「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。

端末

- ☐ Application Controlがプロセスをブロックしました
- ☐ Application Controlが既知の脅威のハッシュリストにあるプロセスをブロックしました
- ☐ スキャンエラー
- ☐ 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
- ☐ 既知の脅威のハッシュによってセキュリティ脅威が検出されました
- ☐ 既知の脅威のハッシュによるセキュリティ脅威の検出に関する予防的保護のレポート
- ☐ 既知の脅威のハッシュによるセキュリティ脅威の検出時にスキャンエラーが発生しました
- ☐ 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
- ☐ 端末が管理者によって承認されました
- ☐ 端末が自動で承認されました
- ☐ 端末の再起動が必要です
- ☐ 端末の認証失敗
- ☐ 端末はすでにログインしています
- ☐ 端末は長い間Serverに接続していません
- ☐ 端末更新のクリティカルエラー
- ☐ 未知の端末
- ☒ 予防的保護のレポート



5.5 Dr.Web Agent 設定の変更

5.5.1 パーミッション設定の変更【推奨】

現在提供している削除ツール(drw_remover.exe)を使用する際には、端末上での Self-Protection の解除が必要となります。下記の設定を実施すると、Self-Protection の解除が可能な状態となります。

- 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) 「パーミッション」をクリックします。
- 4) 「Windows」タブ内の「全般」タブを開きます。
- 5) 「Self-Protection を無効にする」にチェックを入れます。
- 6) 「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。

【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。

5.5.3 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。そのようなことを防止するため、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。

5.6 Dr.Web インストールパッケージの追加

Dr.Web Agent for Windows 以外のインストーラを、下記 URL からダウンロード可能にする場合、インストールパッケージを追加する必要があります。

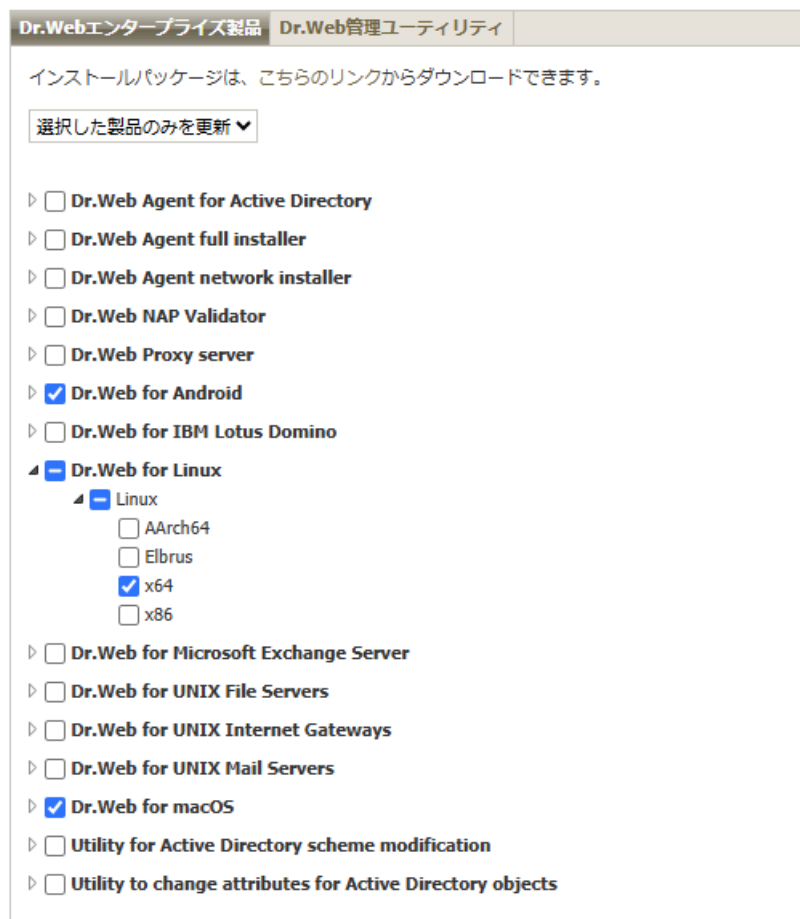
`http://<ESS サーバの IP アドレス or DNS 名>:9080/install/`

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

尚、Dr.Web for Android、Dr.Web for Linux、Dr.Web for macOS のインストールパッケージを追加した場合には、CC 上で端末個別のインストーラやグループインストールパッケージとしてダウンロード可能です。

- 1) CC にログインし、「管理」メニューを開きます。
- 2) 「リポジトリ一般設定」をクリックします。
- 3) 「Dr.Web インストールパッケージ」タブ内の「Dr.Web エンタープライズ製品」タブを開きます。
- 4) 「選択した製品のみを更新」が選択されていることを確認し、必要なインストールパッケージを選択します。

※ 下図では、Dr.Web for Android、Dr.Web for Linux(x64)、Dr.Web for macOS を選択しています。



Dr.Webエンタープライズ製品 Dr.Web管理ユーティリティ

インストールパッケージは、こちらのリンクからダウンロードできます。

選択した製品のみを更新 ▼

- ☐ Dr.Web Agent for Active Directory
- ☐ Dr.Web Agent full installer
- ☐ Dr.Web Agent network installer
- ☐ Dr.Web NAP Validator
- ☐ Dr.Web Proxy server
- ☒ Dr.Web for Android
- ☐ Dr.Web for IBM Lotus Domino
- ☒ Dr.Web for Linux
 - ☒ Linux
 - ☐ AArch64
 - ☐ Elbrus
 - ☒ x64
 - ☐ x86
- ☐ Dr.Web for Microsoft Exchange Server
- ☐ Dr.Web for UNIX File Servers
- ☐ Dr.Web for UNIX Internet Gateways
- ☐ Dr.Web for UNIX Mail Servers
- ☒ Dr.Web for macOS
- ☐ Utility for Active Directory scheme modification
- ☐ Utility to change attributes for Active Directory objects

- 5) 「保存」ボタンをクリックします。
- 6) 再度「Dr.Web インストールパッケージ」タブ内の「Dr.Web エンタープライズ製品」タブを開き、4)で選択したパッケージにチェックがついていることを確認します。

※ リポジトリの更新が実行された後に、利用可能となります。



5.7 Dr.Web 管理ユーティリティの追加【推奨】

Dr.Web for Windows 削除ユーティリティ(drw_remover.exe)は、CC 上で管理ユーティリティとして追加することにより、CC の「管理」メニューの「ユーティリティ」からダウンロード可能となります。

※ 2025 年 3 月 19 日時点では、Dr.Web for Windows 削除ユーティリティ(drw_remover.exe)を、Doctor Web のホームページからダウンロードすることはできません。

- 1) CC にログインし、「管理」メニューを開きます。
 - 2) 「リポジトリ一般設定」をクリックします。
 - 3) 「Dr.Web インストールパッケージ」タブ内の「Dr.Web 管理ユーティリティ」タブを開きます。
 - 4) 「選択した製品のみを更新」が選択されていることを確認し、「Dr.Web for Windows removal utility」を選択します。
- ※ 下図では、Dr.Web for Windows removal utility(Dr.Web for Windows 削除ユーティリティ、drw_remover.exe)、Dr.Web utility for collecting information on a system(Windows 用ログ取得ツール、dwsysinfo.exe)を選択しています。



- 5) 「保存」ボタンをクリックします。
 - 6) 再度「Dr.Web インストールパッケージ」タブ内の「Dr.Web 管理ユーティリティ」タブを開き、4)で選択したパッケージにチェックがついていることを確認します。
- ※ リポジトリの更新が実行された後に、CC の「管理」メニューの「ユーティリティ」からダウンロード可能となります。



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。包括的保護のライセンスが適用されている場合の初期状態は以下となっております。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 Agent Scanner for Windows	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



【注意】最新の"Dr.Web Anti-spam"は、Windows XP(および Windows Server2003)には対応していません。
Windows XP(および Windows Server2003)の端末には、"Dr.Web Anti-spam"をインストールしないようにしてください。

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[レポジトリ一般設定]-[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、Office Control 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>

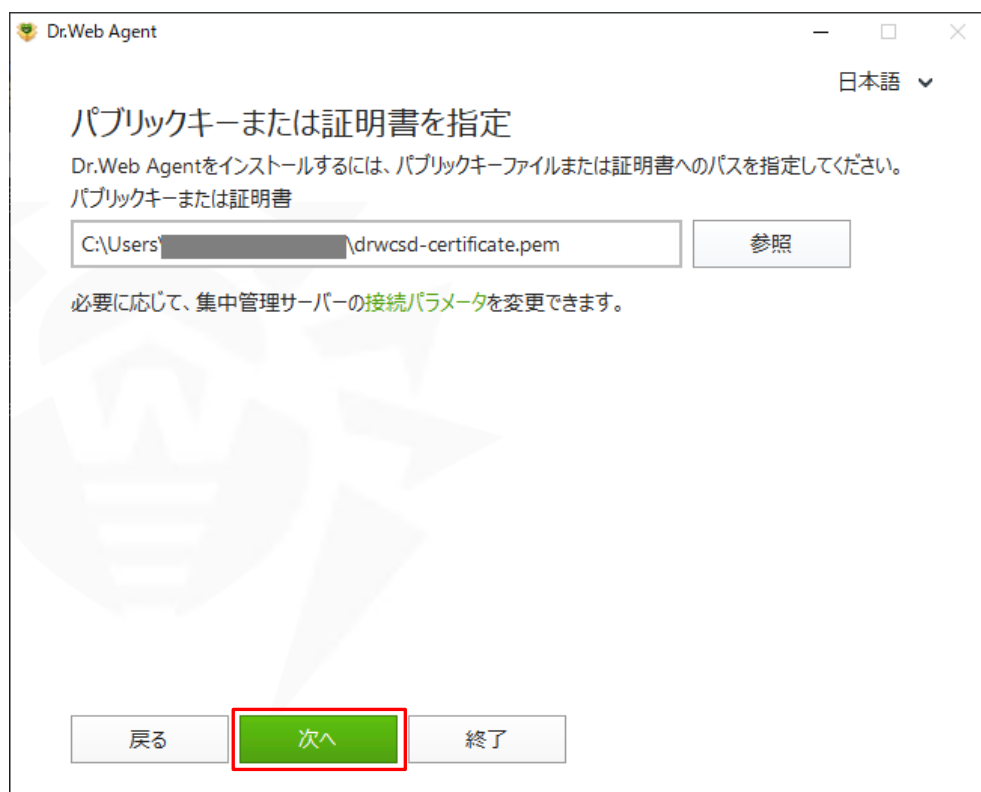
ファイル名 : drwcsd-certificate.pem

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。



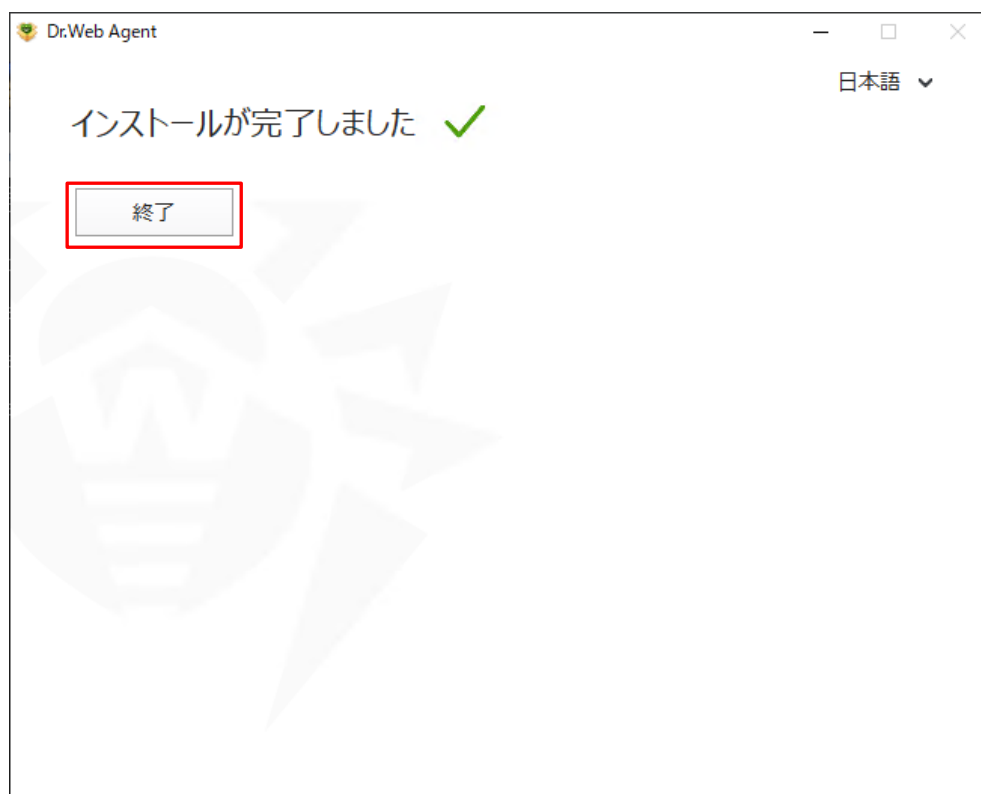
- 3) 以下の画面で暗号化キーが指定されていることを確認して、「次へ」をクリックします。



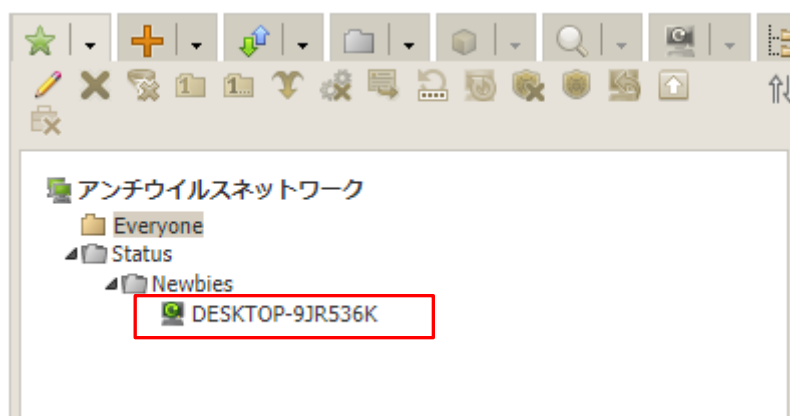
- 4) しばらくすると、以下の画面が表示されるので、「インストール」をクリックします。



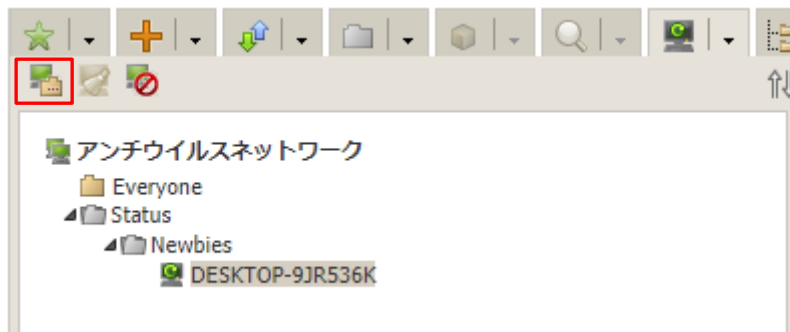
- 5) 以下の画面が表示されたら、「終了」をクリックします。



- 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。



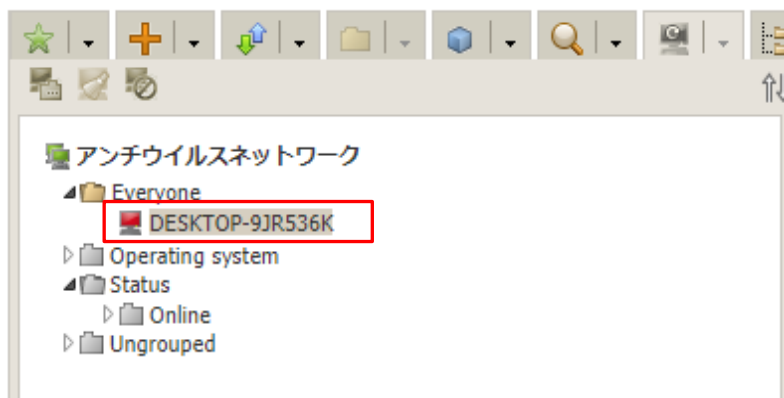
- 8) インストールした端末(以下の図では、DESKTOP-9JR536K)を選択し、「選択した端末を承認し、プライマリグループを設定」ボタンをクリックします。



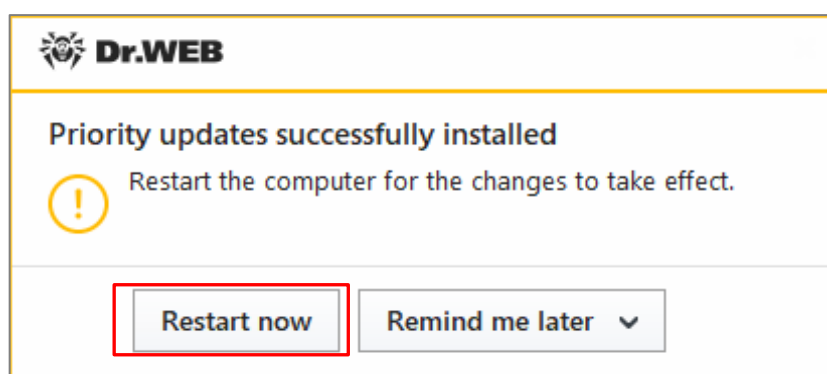
- 9) 画面右側から「プライマリグループ」を選択し、「保存」ボタンをクリックします。



- 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

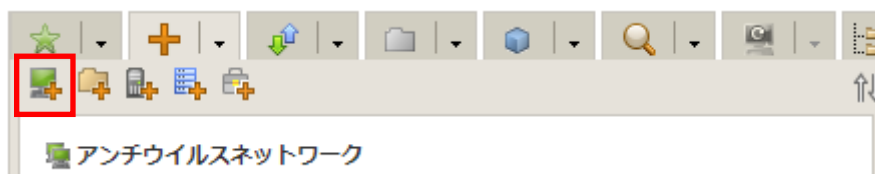
端末(Agent)毎に専用のインストーラを作成します。これを用いると、サーバ上での承認が不要となります。インストール完了後には、再起動を実施してください。

※ 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。

新規端末

保存

全般

端末数*

1

ID*

38309751-a3db-4bd3-82d8-75d1ba0a5016

名前*

新規端末

パスワード

パスワードの確認

説明

グループ

メンバーシップ

☒ Everyone
 ☐ Test001
 ☐ Test002

※ 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。

端末の作成

インストール

38309751-a3db-4bd3-82d8-75d1ba0a5016

インストールファイル

設定ファイル

パスワード

38309751-a3db-4bd3-82d8-75d1ba0a5016端末は正常に作成されました。

Windows

macOS & Android & Linux

.....

- 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。

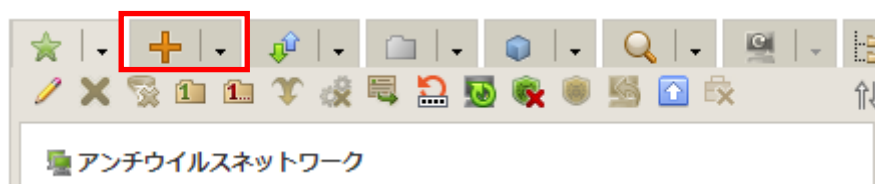
- 2) [Dr.Web Server の設定]-[全般]を開きます。

- 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。

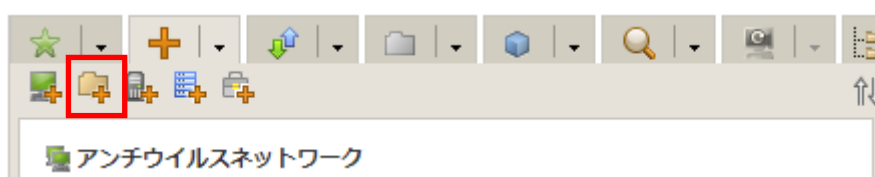
※ 再起動要求が表示された場合、再起動ボタンをクリックして再起動してください。

- 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。

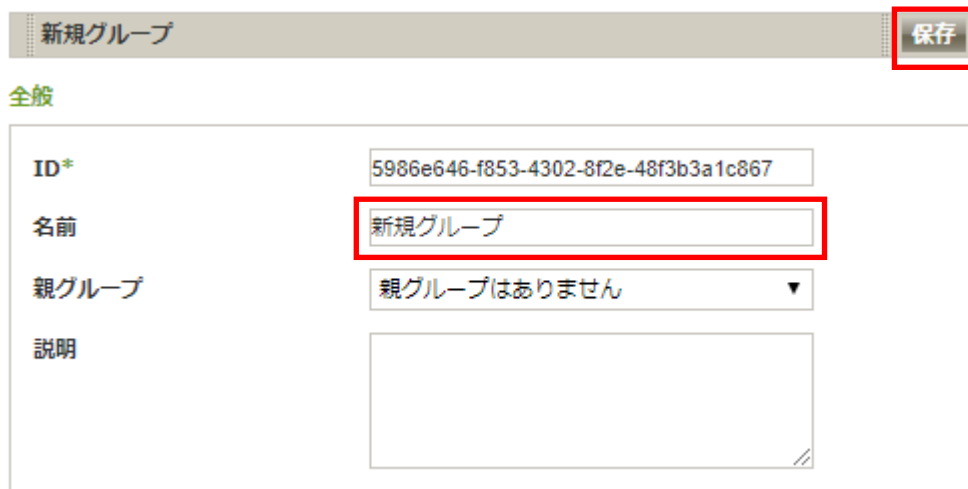


- 6) 次にフォルダのアイコンをクリックします。



7) 「新規グループ」の箇所、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。



新規グループ

保存

全般

ID* 5986e646-f853-4302-8f2e-48f3b3a1c867

名前 新規グループ

親グループ 親グループはありません ▼

説明

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フルパッケージ

インストーラの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。

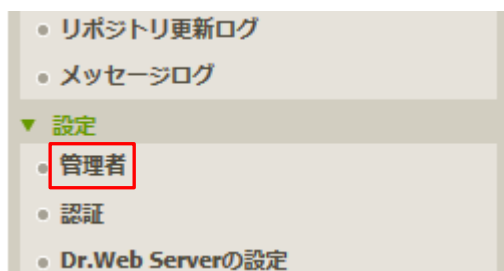
- 4) PC の再起動中に 6-2-2 の 6)~10) の手順を実行します。

※ 必ず、端末を CC 上で承認してください。

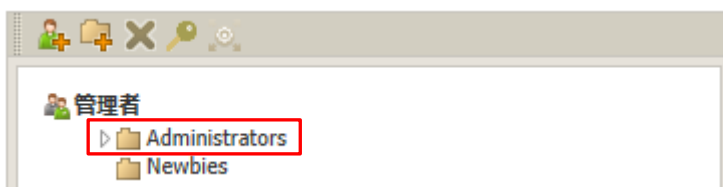
7. ケーススタディ

7.1 管理者(admin)パスワードの変更

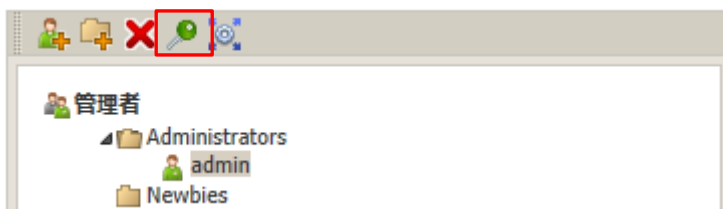
- 1) CC にログインします。
- 2) 「管理」メニューに移動します。
- 3) [設定]-[管理者]をクリックします。



- 4) 画面中央のツリーから「Administrators」を展開します。

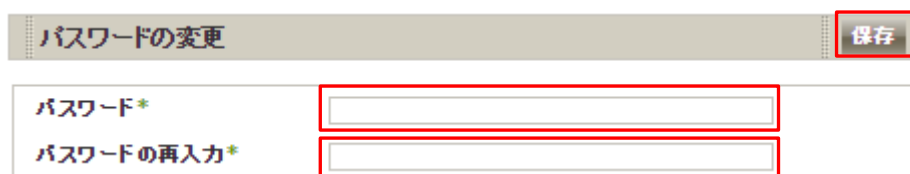


- 5) 「admin」を選択し、「パスワードの変更」アイコンをクリックします。



※ 「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。

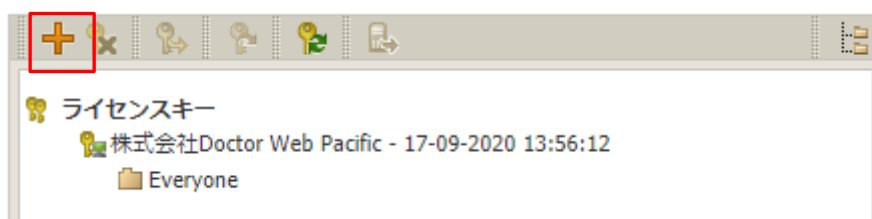
- ※ ESS12 では、ESS10 や ESS11 と同様に一つのグループに複数のライセンスキーを紐づけたり、逆に一つのライセンスキーに複数のグループを紐づけたりすることが可能です。ライセンスキーとグループは、1 対 1 ではなく、n 対 n の関係となります。
- ※ 複数のライセンスがある場合、Everyone グループに割り当てたライセンス以外を特定のグループに紐づけることも可能です。ライセンスが紐づけられたグループをプライマリグループとして設定されている端末に、配信されます。

- 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。

管理 ☆



- 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。

新しいキー 保存

ファイル選択

Agent.key Q

☒ Everyoneグループのライセンスキーを置き換える

- 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。

インストールするコンポーネントの設定を編集 X

保存

キーの置き換え後に個人設定を変更する端末およびグループを選択してください

	現在のキー	割り当てるキー
☒  Everyone	株式会社Doctor Web Pacifi...	株式会社Doctor Web Pacifi...

☒ 異なるもののみを表示

- ※ 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。

インストールするコンポーネントの設定を編集 X

保存

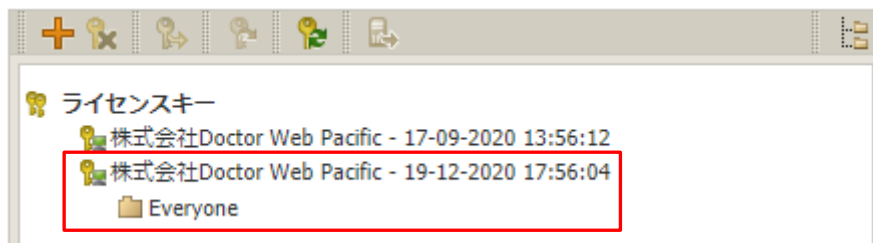
インポートされたキーで指定されている、インストールコンポーネントのリストは、現在のキーのリストとは異なります

キーの置き換え後に、インストールしたコンポーネントの個人設定をセットする端末およびグループを選択してください

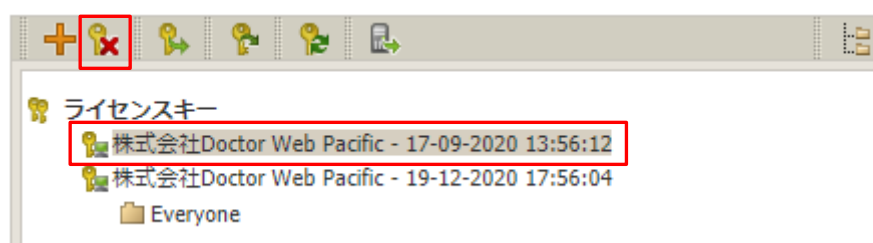
	現在のキー	割り当てるキー
☒  Everyone	株式会社Doctor Web P...	株式会社Doctor Web P...
SpIDer Guard for Windows servers	インストール可能	インストール不可能

☒ 異なるもののみを表示

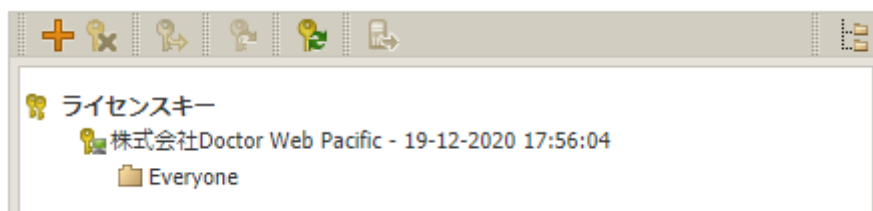
- 9) 画面中央の「ライセンスキー」ツリーに追加したライセンスの「登録名」と「ライセンス終了日」が表示されたこと、「Everyone」グループが紐づいたことを確認します。



- 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 Dr.Web Agent for Windows 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>
```

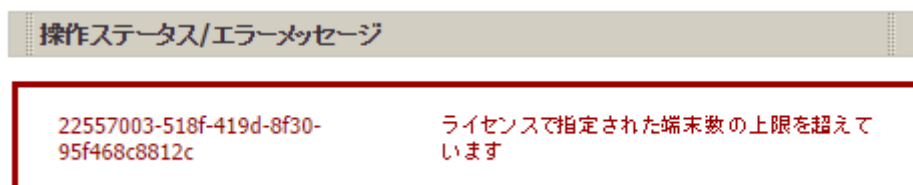
7.4 Dr.Web Agent for Windows の言語の変更

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、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。

7.8 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。

全般	モビリティ	ログ	インターフェース	イベント
☒ タスクバーにアイコンを表示				 
☒ コンポーネントの更新時に再起動要求を表示する				 
☒ 重要な通知				 
☒ 脅威に関する通知				 

- 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。

		①	②	③	④	⑤	⑥									
		本日				13-11-2019 00:00:00	13-11-2019 23:59:59	リフレッシュ								
端末	コンポーネント															
ESS12-AGENT	Dr.Web Scanner for Windows	14	4	0	0	0	0	0	4	0	0	0	26870			
ESS12-AGENT	SpIDer Mail for Windows	0	0	0	0	0	0	0	0	0	0	0	0			
ESS12-AGENT	SpIDer Gate for Windows workstations	138	0	0	0	0	0	0	0	1	0	0	0			
ESS12-AGENT	SpIDer Guard for Windows workstations	995	5	0	0	0	0	0	5	0	0	0	3692438.69			

1

ページ: 1

1~4/ 4を表示中 10

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。

最も感染している端末									
ESS12-AGENT 9									
最も多く検出された脅威									
JS.Downloader.3943 4									
Mac.Trojan.KeRanger.1 2									
Mac.Trojan.KeRanger.2 2									
BackDoor.Bebloh.177 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	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\170611\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。

Ver	プログラム, ドキュメント	
12.0	Dr.Web Enterprise Security Suite server 選択して下さい ▼ Windows OS向けエージェントインストーラフルパッケージ drweb-12.00.0-201910280-esuite-agent-full-windows.exe Dr.Web Repository Loader 選択して下さい ▼	Administrator's Guide 日本語 ▼ ダウンロード (PDF形式) Anti-virus Network Quick Installation Guide 日本語 ▼ ダウンロード (PDF形式) インストールマニュアル 日本語 ▼ ダウンロード (PDF形式)

- ※ 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。

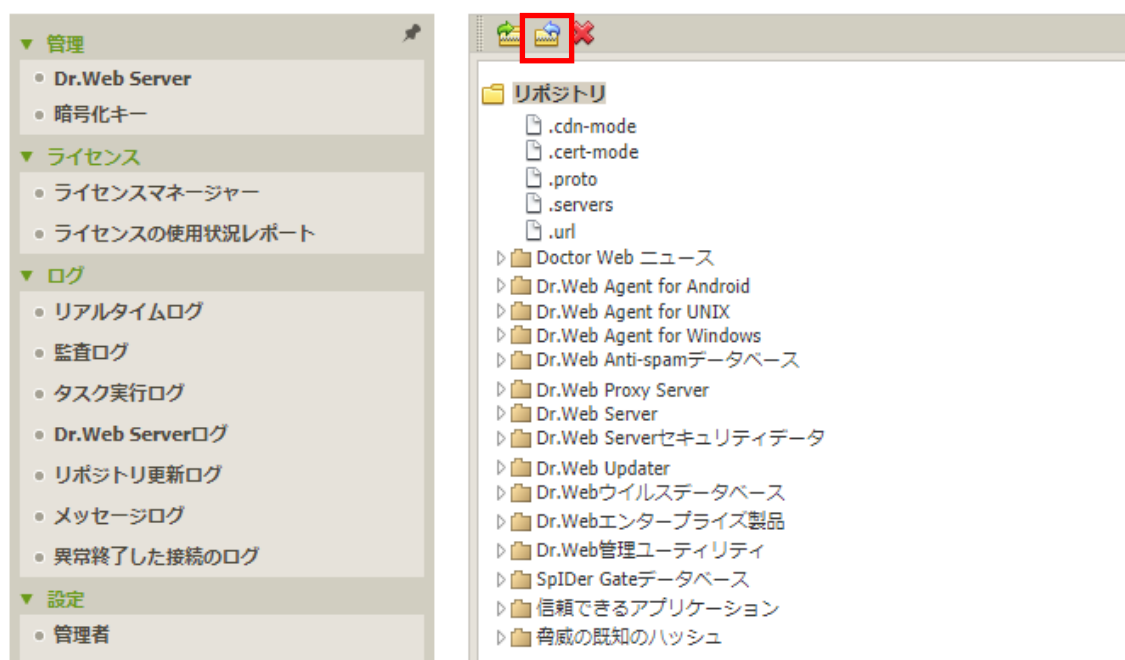


- 6) 下記が表示されたら「OK」ボタンをクリックし、保存された zip ファイルを USB メモリ等にコピーします。

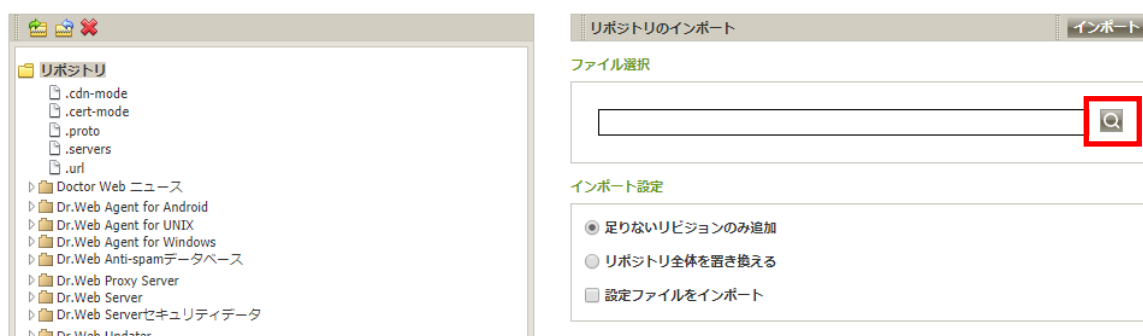


- 7) クローズドネットワーク内の CC にログインします。
8) 「管理」メニューから「レポジトリコンテンツ」を開きます。
9) 「リポジトリファイルを含んだアーカイブをインポート」アイコンをクリックします。

管理 > リポジトリコンテンツ ☆



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。



7.14 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、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」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。

7.14.2 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。

Dr.Web Proxy Server

☐ リンクされたDr.Web Proxy Serverを作成

- 5) 必要事項を入力した後、「保存」をクリックします。

Dr.Web Proxy Server

☒ リンクされたDr.Web Proxy Serverを作成

ID*

名前*

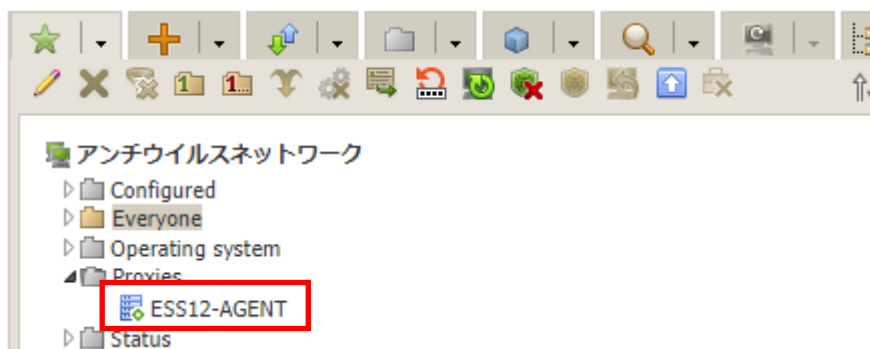
パスワード

パスワードの確認

メンバーシップ

▷ ☒ Proxies

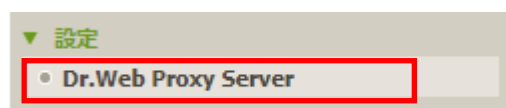
- 6) 「アンチウイルスネットワーク」メニュー中央のツリー内に「Proxies」グループ配下に追加したプロキシサーバーが表示されたことを確認します。
- 7) しばらく待ち、プロキシサーバーのアイコンの状態が水色に変わったことを確認します。



7.14.3 Dr.Web Proxy の設定変更

7.14.2 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

リダイレクト先アドレス	暗号化	圧縮	圧縮レベル	管理Server
centos7.staging	可能であれば	可能であれば	8 (最適)	いいえ

- 4) 「この Server から Dr.Web Proxy Server の設定を管理することができます」を「はい」に変更し、次の項目を設定した後、「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。

Dr.Web Server との接続設定を変更する

このServerからDr.Web Proxy Serverの設定を管理することができます

リダイレクト先アドレス

暗号化

圧縮

圧縮レベル

はい

192.168.1.151

いいえ

いいえ

8 (最適)

更新 インストール

同時更新プロセス数

1

☐ 更新トラフィックを制限する

トラフィック帯域幅の上限 (KB)

1

00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23

月

火

水

木

金

土

日

保存

- 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
192.168.1.151	いいえ	いいえ	8 (最適)	はい

- 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。

Proxies. カスタム設定が指定されました

証明書 待ち受け (リスン) **キャッシュ** イベント ダンプ DNS 検索 更新

☒ キャッシュを有効にする

リビジョンの削除間隔 (分)

残るリビジョンの数

使われていないファイルをアンロードする間隔 (分)

整合性チェックモード

☒ プロアクティブキャッシングを使用する

- ☒ Dr.Web Agent for Windows
- ☒ Dr.Web Agent for UNIX
- ☒ Dr.Web Agent for Android
- ☒ Dr.Web Proxy Server
- ☒ Dr.Web Updater
- ☒ Dr.Webウイルスデータベース
- ☒ SpIDer Gateデータベース
- ☒ Dr.Web Anti-spamデータベース
- ☒ 信頼できるアプリケーション
- ☒ 脅威の既知のハッシュ
- ☐ Dr.Webエンタープライズ製品
- ☐ Dr.Web管理ユーティリティ

- 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。

```
C:\> 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:\> _
```

7.15 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。

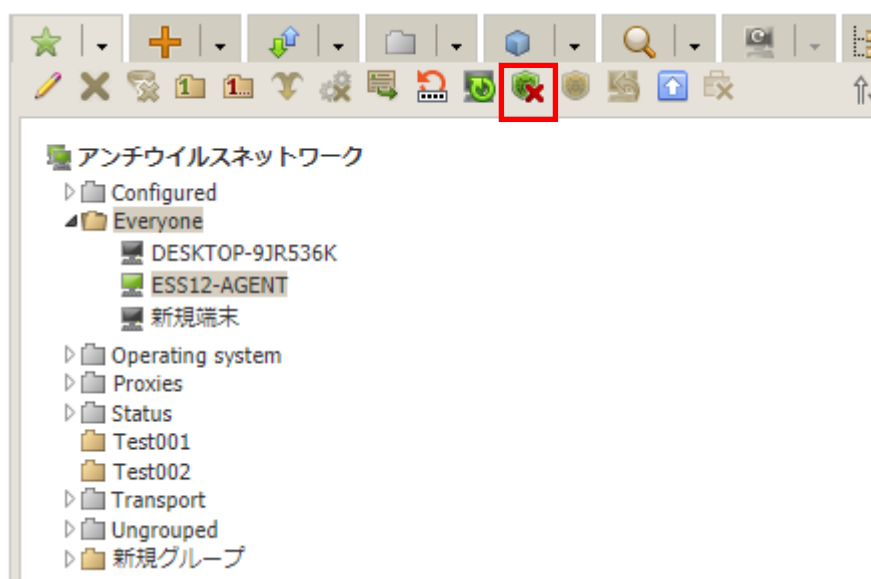
- CC 上から
- クライアント PC 上から

※ 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。

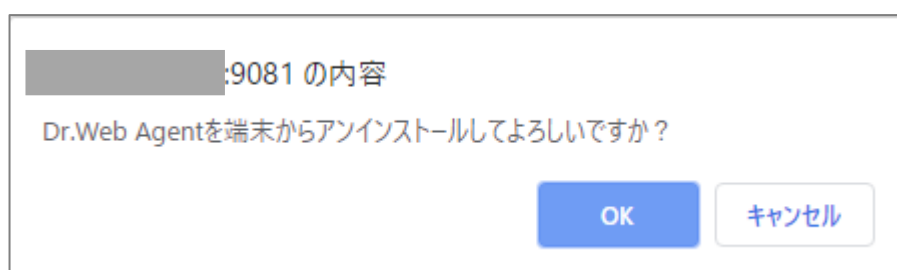
7.15.1 CC 上からのアンインストール

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。

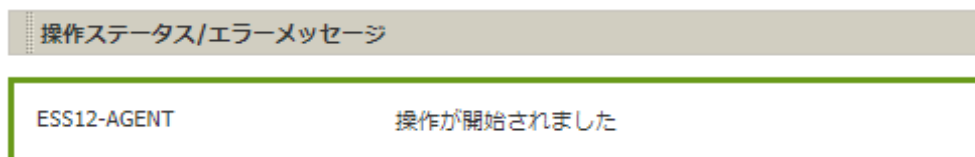
- 1) CC にログインします。
- 2) 「アンチウイルスネットワーク」メニュー中央のツリーから対象の端末を選択します。
- 3) ツリー上部の全般アイコン(星型のアイコン)をクリックし、下図の赤枠のアイコン(Dr.Web のアイコンに赤い×印がついたアイコン)をクリックします。



- 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。

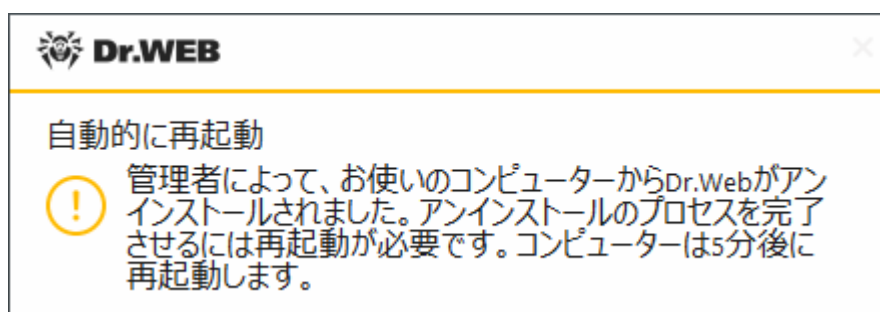


- 5) 以下のような表示がされたことを確認します。

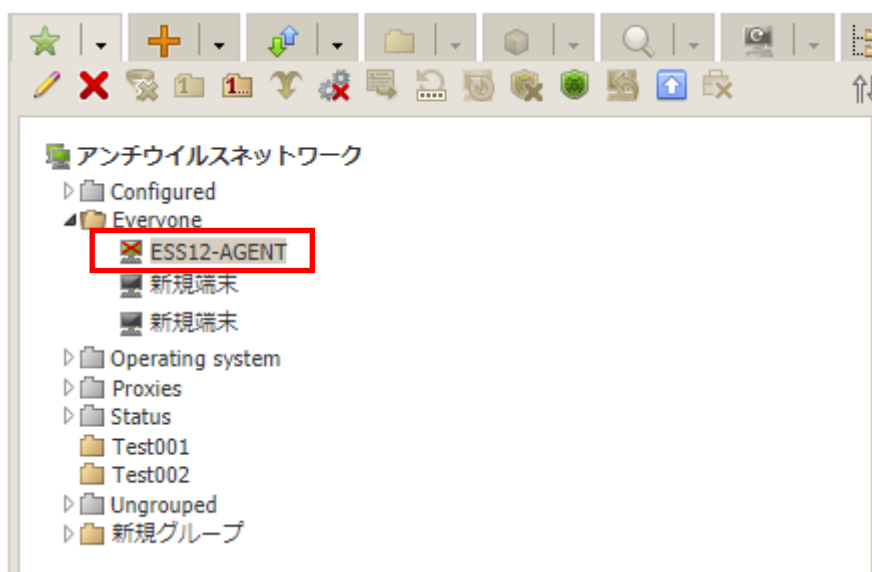


- 6) クライアント PC 上に以下のようなメッセージが表示されたら、PC を再起動してください。

※ 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。

7.15.2 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
```

※ 「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。

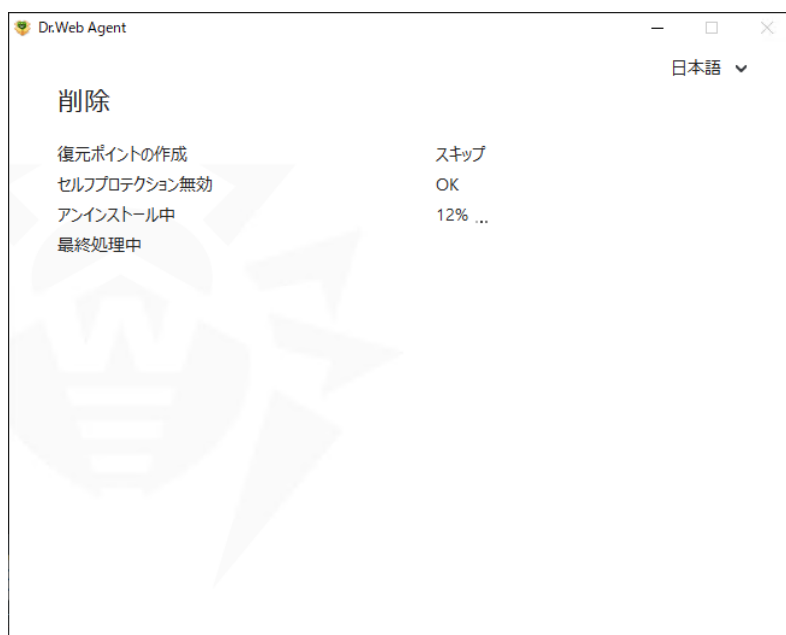
- 3) 以下の画面で「次へ」をクリックします。



- 4) 以下の画面で「削除」をクリックします。



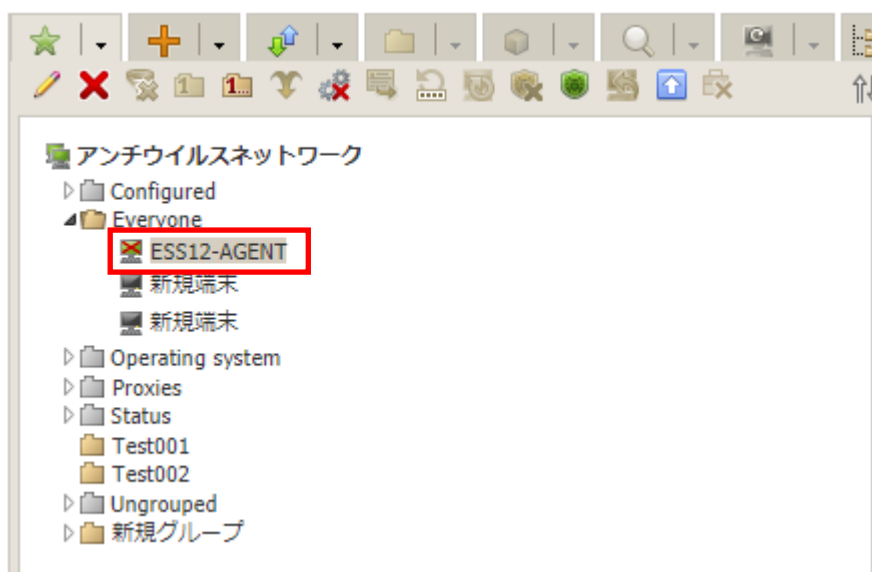
- 5) アンインストールが開始します。



- 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。

7.15.3 アンインストールに失敗する場合の対処

7.15.1 および 7.15.2 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、Dr.Web for Windows 削除ユーティリティ(drw_remover.exe)ご利用ください。

Dr.Web for Windows 削除ユーティリティ(drw_remover.exe)は、「5.7 Dr.Web 管理ユーティリティの追加」の手順を実施していただくと、CC 上からダウンロード可能となります。

※ 2025 年 3 月 19 日時点では、Dr.Web for Windows 削除ユーティリティ(drw_remover.exe)を、Doctor Web のホームページからダウンロードすることはできません。

Dr.Web for Windows 削除ユーティリティ(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、Dr.Web for Windows 削除ユーティリティ(drw_remover.exe)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。

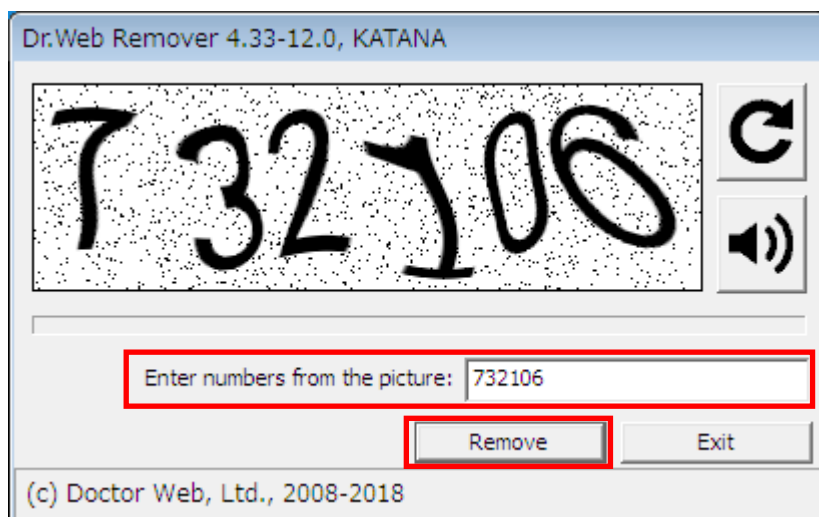
- 1) CC の「管理」メニューの「ユーティリティ」から Dr.Web for Windows 削除ユーティリティ(drw_remover.exe)をダウンロードします。

※ "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。

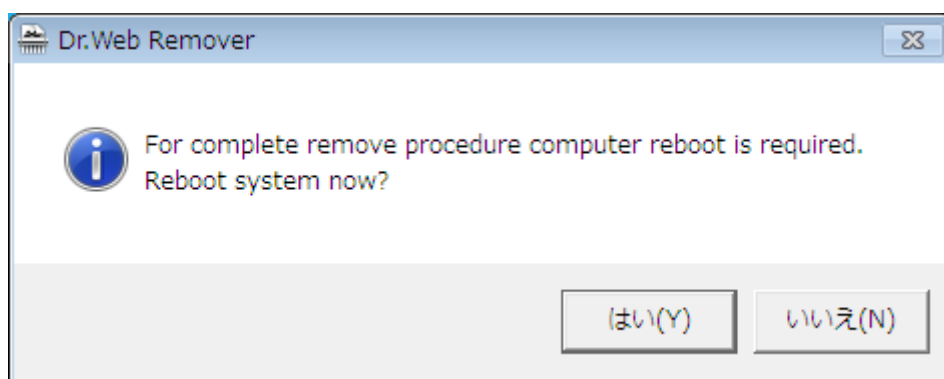
- 2) 端末上で Self-Protection を無効にします。
- 3) ダウンロードした"drw_remover.exe"を実行します。

※ 「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/>

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