



---

# Dr.Web Enterprise Security Suite Ver.13 簡易構築ガイド -Linux 用-

株式会社 Doctor Web Pacific

初版 : 2022/01/28

改訂 : 2023/09/12

## 目次

1.	はじめに.....	4
1.1	ライセンス情報の受領.....	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	ライセンスの登録と表示言語の変更.....	7
5.	Control Center の設定.....	11
5.1	リポジトリの更新【必須】.....	11
5.2	ESS サーバの更新【必須】.....	11
5.3	「Dr.Web Server の設定」の変更.....	11
5.3.1	サーバアドレスの設定【必須】.....	11
5.3.2	暗号化設定(サーバ側)の変更.....	12
5.3.3	Server 言語の変更.....	12
5.3.4	Server のログ設定の変更.....	12
5.4	「Web サーバーの設定」の変更.....	13
5.4.1	サーバアドレスの変更【必須】.....	13
5.4.2	https へのリダイレクトの停止設定.....	13
5.5	管理者パスワードのリセット機能の有効化.....	13
5.5.1	メールサーバの設定.....	13
5.5.2	管理者用メールアドレスの登録.....	13
5.6	「通知設定」の変更【推奨】.....	14
5.7	Dr.Web Agent 設定の変更・確認.....	15
5.7.1	パーミッション設定の変更【推奨】.....	15
5.7.2	Dr.Web for Microsoft Outlook の設定確認【必須】.....	15
5.7.3	SpIDer Mail の設定確認【必須】.....	15
5.7.4	hosts の除外設定【推奨】.....	16
5.7.5	Windows8、Windows10、Windows11 使用時の設定変更.....	16
5.8	Dr.Web インストールパッケージの追加.....	17
6.	Dr.Web Agent for Windows のインストール.....	18



6.1	Dr.Web Agent for Windows のインストールの前に.....	18
6.1.1	導入するコンポーネントの選択 .....	18
6.1.2	その他(注意事項等).....	19
6.2	Dr.Web Agent for Windows のインストーラの配布とインストール、承認.....	21
6.2.1	Dr.Web Agent for Windows のインストーラの配布 .....	21
6.2.2	Dr.Web Agent for Windows のインストール、承認 .....	21
6.3	その他の Dr.Web Agent for Windows のインストール方法 .....	25
6.3.1	端末毎の専用インストーラ.....	25
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	PC のクローニングについて .....	37
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 .....	37
7.8.2	構築済みの ESS サーバはあるが、イメージ展開時に通信が不可能な場合 .....	38
7.8.3	構築済みの ESS サーバがない場合 .....	38
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.....	39
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 .....	40
7.11	統計情報.....	41
7.11.1	スキャン統計情報 .....	41
7.11.2	脅威.....	42
7.12	Dr.Web Agent for Windows のアンインストール .....	43
7.12.1	Dr.Web Agent for Windows のアンインストール.....	43
7.12.2	アンインストールに失敗する場合の対処.....	48



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 サーバ、Dr.Web Server/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。

➤ 製品マニュアル

<https://download.drweb.co.jp/doc/>

## 1. はじめに

### 1.1 ライセンス情報の受領

ライセンス情報(シリアル番号)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。

ライセンス情報(シリアル番号)を受領した後は、下記 URL よりライセンスの有効化を実施し、ライセンスキーファイルを取得してください。

<https://products.drweb.co.jp/register/v4/>

※ “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。

➤ Oracle Linux 8.5 (64bit)

➤ firewalld は無効

※ firewalld を有効な状態で利用される場合には、通信に利用するポート(2193/tcp、2193/udp、9080/tcp、9081/tcp)の開放が必要となります。

➤ 2023 年 7 月 20 日時点での最新のインストーラを使用

➤ Enterprise Security Suite (以降、ESS)サーバ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ことを確認してください。

TCP : 2193, 139, 445

UDP : 2193, 139, 445

http : 80, 9080

https : 443, 9081

➤ IP アドレス

ESS サーバをインストールするサーバ(または端末)に固定 IP アドレスが付与されているか確認してください。

DHCP 設定となっている場合には、設定を変更してください。

➤ モジュール等

ESS サーバをインストールするサーバ(または端末)に、SysVinit がインストールされていることを確認してください。インストールされていない場合には、追加してください。

ESS サーバをインストールするサーバ(または端末)の glibc が v.2.13 以降であることを確認してください。

※ メモリ、HDD 容量等については、製品マニュアルページ内の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 に対応した.run ファイルを用意し、インストール対象のサーバ(または端末)にコピーしてください。

➤ ライセンスキーファイル(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.

:
```

※ バックアップデータを指定する箇所となりますが、新規インストールのため「0」を入力します。

※ 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。

- 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.
Log is written to file /<ログの保存フォルダ>/<日時>.install.log
#
```

※ 上記の例では、赤字で示した"7DRh9GbGeA"がパスワードとなります。

**【重要】**パスワードは、ランダムに生成されるため**必ず記録**してください。以前のバージョンとは異なり、パスワードを確認する方法はありません。

パスワードを紛失した場合には、以下のコマンドを実行して admin のパスワードを再設定してください。

```
# /etc/init.d/drwcsd modexecdb set-admin-password admin 新しいパスワード
```



- 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。

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

#### 4.3 ライセンスの登録と表示言語の変更

インストールが完了したら、管理画面(Control Center)へログインし、表示言語の変更とライセンスの登録を行います。

- 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/

※ 初期状態では、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 にログインします。

Login

Password

Reset password

Log in

ID : admin

Password : インストールの最後に表示されたもの

※ インストール直後の状態では、メールサーバの設定が行われていないため"Reset password"(または「パスワードをリセット」)を使用することはできません。

- 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。

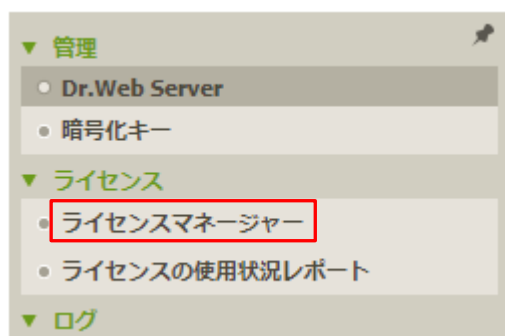
#### General

Identifier	c9687f73-d21d-b211-a797-85419c46f0e6
Login*	admin
Authentication type	Internal
First name	
Middle name	
Last name	
Email address	
Interface language	English ▼
Date format	DD-MM-YYYY HH:MM:SS ▼
Time zone	Nothing is selected ▼
Last address	https://192.168.1.125:54632:31
Creation date	21-07-2023 13:44:03
Modification date	21-07-2023 13:44:03
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。





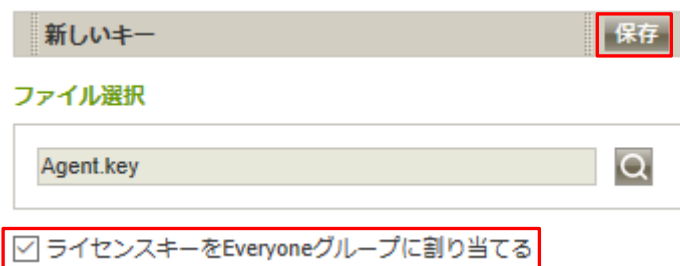
- 8) 画面中央の「ライセンスキー」と書かれたツリーの上にある「ライセンスキーを追加」アイコンをクリックします。



- 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) 予め用意してあるライセンスキーファイル(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。

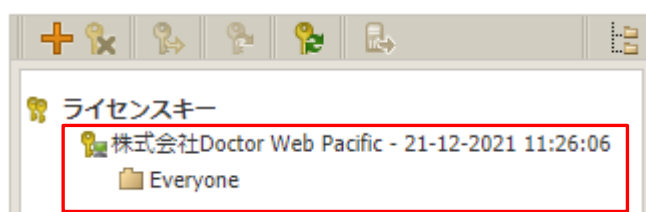


- 12) 以下のような画面が表示されるので、必要に応じて設定を変更し「保存」ボタンをクリックします。



※ 登録するライセンスによっては、画面の表示が上記とは異なることがあります。

- 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。



※ 以下のようなメッセージが表示される場合がありますが、ライセンスが未登録の状態から変更されたことによるものです。

操作は正常に終了しました  
新しいキーのコンポーネント数と、以前のキーのコンポーネント数が一致しません。正常な動作のために、新しいキーが割り当てられるオブジェクトの権限を確認してください。

## 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 リポジトリの更新【必須】

- 1) Control Center 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、「リポジトリの更新ログ」を開き、正常に更新されたことを確認します。

**【重要】**「更新情報のチェック」ボタンをクリックした後、ステータスに「更新エリアの証明書が無効か、または信頼できません」と表示された場合や「リポジトリの更新ログ」に「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、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。

※ 正常に更新されたことを確認した後、再度「更新受信プロトコル」を「HTTPS」に変更してください。

### 5.2 ESS サーバの更新【必須】

リポジトリの更新後に 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) Control Center にログインし、「管理」メニューを開きます。
- 2) 「Dr.Web Server」をクリックし、「バージョンリストを表示」のリンクをクリックします。
- 3) アップデートがある場合、「利用可能な更新」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。

※ アップデートは、環境によって異なりますが、数分～数十分かかります。

- 4) アップデート完了後、再度 Control Center 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。

### 5.3 「Dr.Web Server の設定」の変更

#### 5.3.1 サーバアドレスの設定【必須】

- 1) Control Center 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。

### 5.3.2 暗号化設定(サーバ側)の変更

管理対象端末に Android 端末がある場合、以下の設定を行なってください。

※ Dr.Web for Android は、暗号化や圧縮が有効な状態では、接続できません。

- 1) Control Center 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。

### 5.3.3 Server 言語の変更

- 1) Control Center 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。

### 5.3.4 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) Control Center 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。

## 5.4 「Web サーバーの設定」の変更

### 5.4.1 サーバアドレスの変更【必須】

- 1) Control Center 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。

### 5.4.2 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) Control Center 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。

## 5.5 管理者パスワードのリセット機能の有効化

管理者パスワードのリセット機能を有効にするには、以下の操作を実施してください。

※ ESS13 ではパスワードは暗号化された状態で保存されるため、パスワードを紛失した場合に対象の管理者アカウントのパスワードを確認する方法はありません。

### 5.5.1 メールサーバの設定

- 1) Control Center 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「E メール」タブをクリックします。
- 4) 「送信者のメールアドレス」およびメールサーバに接続するために必要な設定を入力します。
- 5) メールサーバに接続するために必要な設定を入力後、「受信者メールアドレス」欄にテストメールを受信するアドレスを入力し、「テストメッセージの送信」をクリックします。
- 6) 指定したアドレスでテストメッセージの受信を確認します。
- 7) 「保存」をクリックし、設定を保存します。
- 8) 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。

### 5.5.2 管理者用メールアドレスの登録

- 1) Control Center にログインし、「環境設定」のアイコンをクリックします。



- 2) 「E メールアドレス」欄に管理者用のメールアドレスを入力し、「保存」ボタンをクリックします。
- 3) 画面から「管理者アカウント設定でメールアドレスを指定してください。この操作を行わない場合、パスワードリセットオプションを使用することができなくなります。」の表示が消えたことを確認します。

## 5.6 「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、その内容はデータベース内に保存されます。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」を、Application Controlを使用されている場合には Application Control に関する項目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
- ☐ 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
- ☐ 端末は管理者によって承認されました
- ☐ 端末は自動的に承認されました
- ☐ 端末は長い間Dr.Web 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



## 5.7 Dr.Web Agent 設定の変更・確認

### 5.7.1 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 の解除が可能となります。

- 1) Control Center 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。

### 5.7.2 Dr.Web for Microsoft Outlook の設定確認【必須】

Microsoft 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、以下の確認を行なってください。

**【注意】**"Dr.Web for Microsoft 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 Microsoft Outlook"を使用するか否かに関わらず、必ず以下の設定の確認は実施してください。

- 1) Control Center 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」の設定が「無視」となっていることを確認します。
- ※ アクションとして「隔離」や「削除」が指定されている場合には、「無視」に変更した後、「保存」ボタンをクリックして設定を保存してください。

### 5.7.3 SpIDer Mail の設定確認【必須】

SpIDer Mail 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、以下の設定の確認を行なってください。

**【注意】**"SpIDer Mail for Windows"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、"SpIDer Mail for Windows"を使用するか否かに関わらず、必ず以下の確認は実施してください。



- 1) Control Center 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) 「SpIDer Mail と SpIDer Gate」をクリックします。
  - 4) 「SpIDer Mail」タブ内の「全般」タブを開きます。
  - 5) 「未検査メッセージ」の設定が「無視」となっていることを確認します。
- ※ アクションとして「隔離」や「削除」が指定されている場合には、「無視」に変更した後、「保存」ボタンをクリックして設定を保存してください。

#### 5.7.4 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) Control Center 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

#### 5.7.5 Windows8、Windows10、Windows11 使用時の設定変更

Windows8、Windows10、Windows11 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) Control Center 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。





## 5.8 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、Control Center 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) Control Center 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、エンタープライズ製品セクションおよびインストールページからダウンロードできます。

選択した製品のみを更新 ▼

- ▷ ☐ Active Directoryオブジェクトの属性を変更するためのユーティリティ
- ▷ ☐ Active Directoryスキーマ変更ユーティリティ
- ▷ ☐ Dr.Web Agent for Active Directory
- ▷ ☐ Dr.Web Agentフルインストーラ
- ▷ ☐ Dr.Web NAP Validator
- ▷ ☐ Dr.Web Proxy Server
- ▷ ☐ Dr.Web Scanning 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

- 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。



## 6. Dr.Web Agent for Windows のインストール

Windows PCにDr.Web Agent for Windows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 Dr.Web Agent for Windows 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

Dr.Web Agent for Windows 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、Control Center 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。

**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 ▼
<hr/>	
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 ▼

※ 上記は、一つのライセンスで Desktop Security Suite(包括的保護)と Server Security Suite をサポートするものが適用されている場合の表示(初期状態)です。

※ “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 Agent Scanner for Windows
- 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

Dr.Web Agent for Windows 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。

- 「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、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。

※ 新規にインストールされた Dr.Web Agent for Windows のコンポーネントは、Control Center 上に保存されている最新のものとなります。

- 「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、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 のコンポーネントが更新されません。

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、プログラムの競合によりホームページの閲覧等ができなくなる場合があります。

その場合は、SpIDer Mail、SpIDer Gate、Dr.Web for Microsoft 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ている場合があると思いますので、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 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 をインストールすると、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「Behavior Analysis」にて新たな保護レベルを追加し、「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 Dr.Web Agent for Windows のインストーラの配布とインストール、承認

### 6.2.1 Dr.Web Agent for Windows のインストーラの配布

Dr.Web Agent for Windows 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、Dr.Web Agent for Windows の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。

➤ Dr.Web Agent for Windows 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

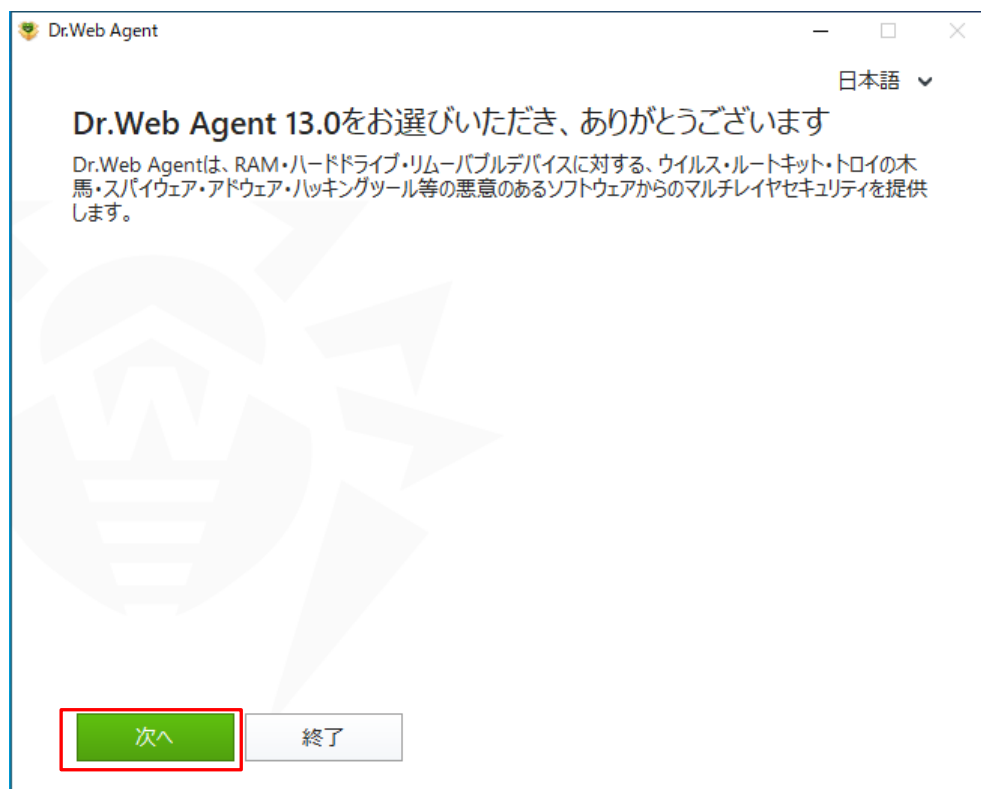
➤ 証明書

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>

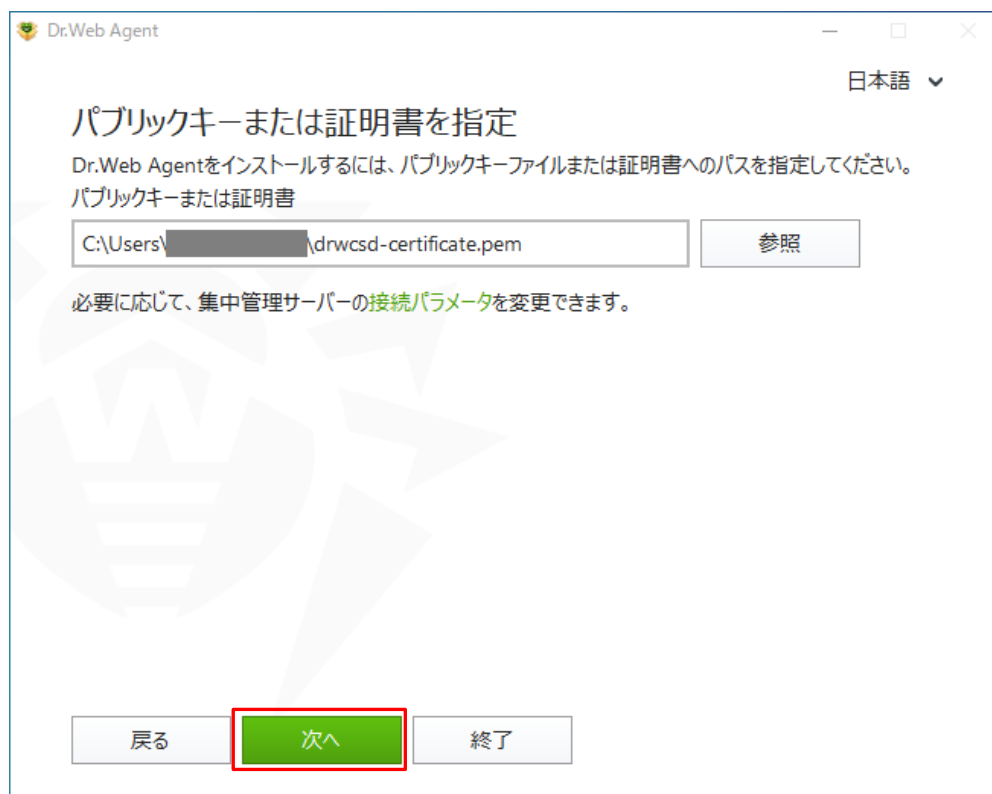
ファイル名 : drwcsd-certificate.pem

### 6.2.2 Dr.Web Agent for Windows のインストール、承認

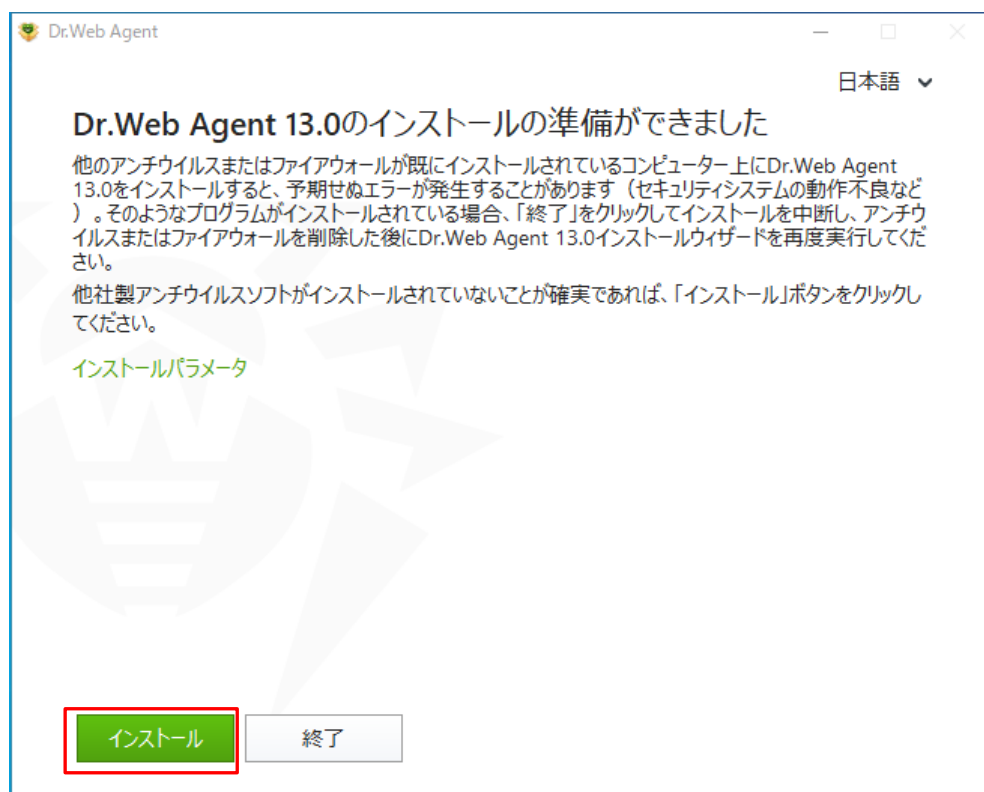
- 1) 端末上に保存した Dr.Web Agent for Windows のインストーラ(drwinst.exe)を実行します。
- 2) 以下の画面が表示されたら、「次へ」をクリックします。



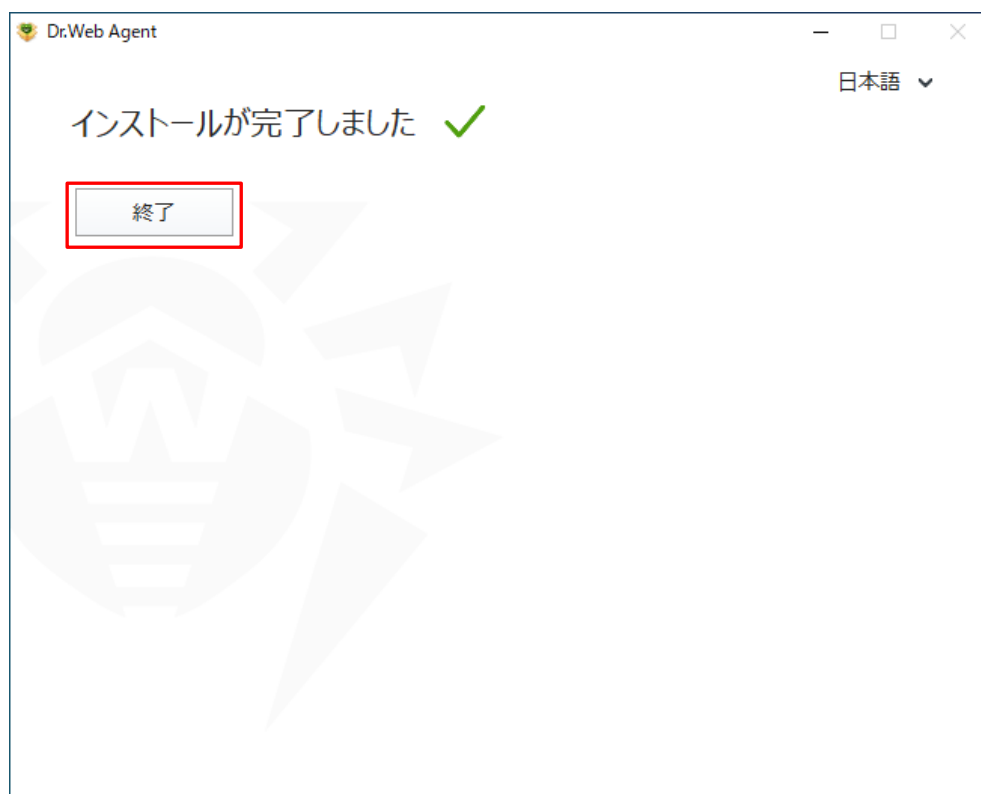
- 3) 以下の画面で暗号化キーが指定されていることを確認して、「次へ」をクリックします。



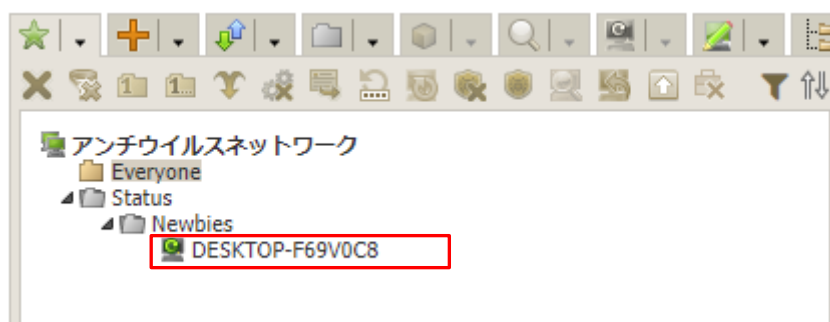
- 4) しばらくすると、以下の画面が表示されるので、「インストール」をクリックします。



- 5) 以下の画面が表示されたら、「終了」をクリックします。



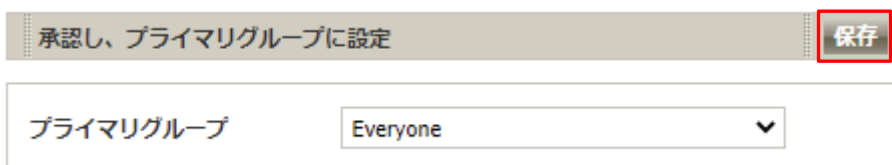
- 6) Control Center にログインし、「アンチウイルスネットワーク」メニューを開きます。
- 7) 画面中央のツリーから、[Status]-[Newbies]を開き、インストールした端末が表示されていることを確認します。



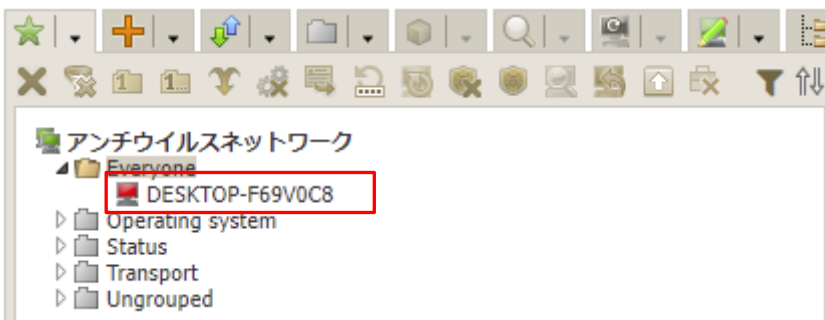
- 8) インストールした端末(以下の図では、DESKTOP-F69V0C8)を選択し、「選択した端末を承認し、プライマリグループを設定」ボタンをクリックします。



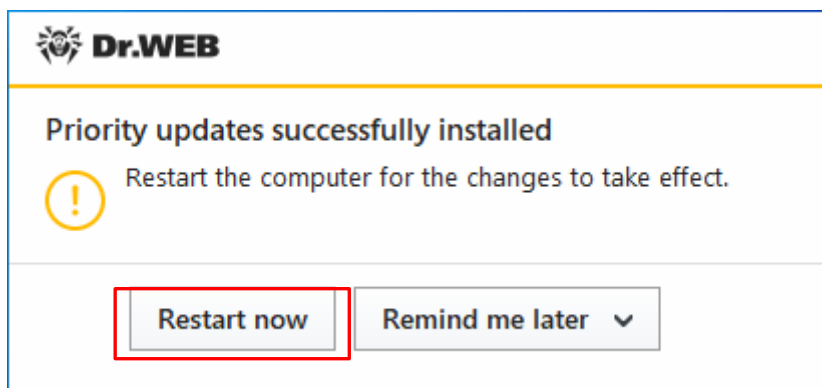
- 9) 画面右側から「プライマリグループ」を選択し、「保存」ボタンをクリックします。



- 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 Dr.Web Agent for Windows のインストール方法

Dr.Web Agent for Windows 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 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

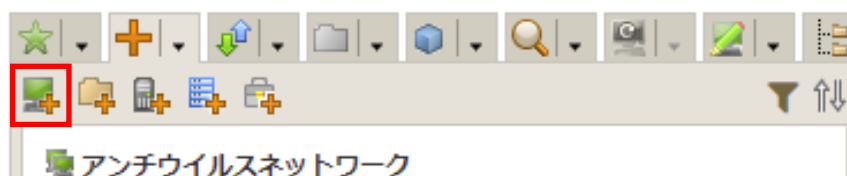
端末(Agent)毎に専用のインストーラを作成します。これを用いると、Control Center 上での承認が不要となります。インストール完了後には、再起動を実施してください。

- ※ インストーラには、端末の識別子(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。
- ※ 端末の識別子(端末 ID、Agent ID)の重複が発生する為、基本的には異なる 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) Control Center 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*	c2926c65-1eb0-4e2c-9850-fe9ca72bf7ce
名前*	新規端末
パスワード	
パスワードの確認	
ブロック期間の開始	不明/時刻設定なし
ブロック期間の終了	不明/時刻設定なし
説明	

グループ

メンバーシップ

編集

☒ Everyone

※ 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) 表示されたメッセージの"詳細"をクリックします。

端末の作成

インストール

操作は正常に終了しました [\(詳細\)](#)

- 6) 「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
操作は正常に終了しました (詳細)		
198b0690-2078-11ee-474e-e8725e7adc65	198b0690-2078-11ee-474e-e8725e7adc65端末は正常に作成されました。	
インストールファイル	<b>Windows</b>	
設定ファイル	macOS & Android & Linux	
パスワード	•	

- ※ 端末(Agent)毎に専用のインストーラは、「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た後、右側に表示された「○○端末のプロパティ」内の「インストールファイル」の"Windows"をクリックし、ダウンロードすることもできます。

新規端末のプロパティ		保存
全般		
端末の識別子 *	198b0690-2078-11ee-474e-e8725e7adc65	
名前 *	新規端末	
作成日	12-07-2023 14:51:14	
パスワード	••••••••	
パスワードの確認	••••••••	
ブロック期間の開始	不明/時刻設定なし	
ブロック期間の終了	不明/時刻設定なし	
MACアドレス		
Dr.WebAgentの最初のダウンロード日	不明/時刻設定なし	
最終接続日	不明/時刻設定なし	
ネットワークアドレス		
OSビルド	Not Found	
説明		
インストールファイル	<b>Windows</b>	
設定ファイル	macOS & Android & Linux	

- 7) 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(drwcds-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。

- 8) 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、Control Center 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) Control Center にログインし、「管理」メニューを開きます。

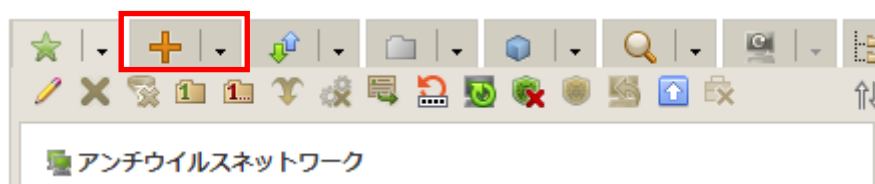
- 2) [Dr.Web Server の設定]-[全般]を開きます。

- 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。

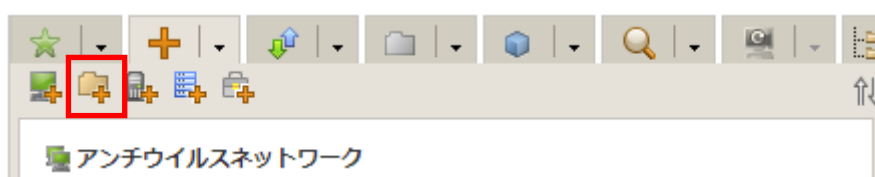
※ 再起動要求が表示された場合、再起動ボタンをクリックして再起動してください。

- 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。

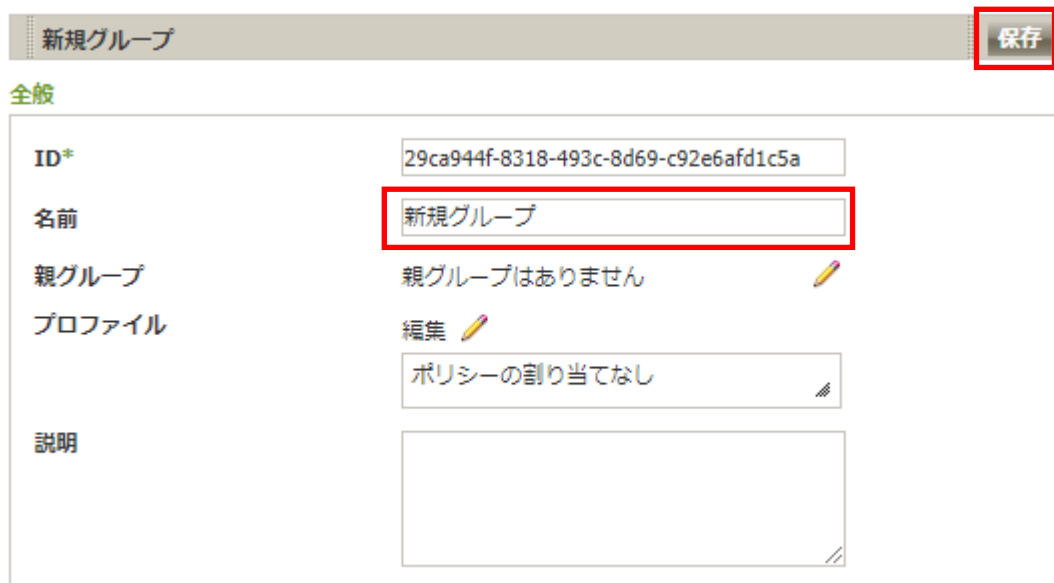


- 6) 次にフォルダのアイコンをクリックします。



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。



The screenshot shows a web interface for creating a new group. At the top, there is a header bar with the text '新規グループ' on the left and a '保存' (Save) button on the right, which is highlighted with a red rectangular box. Below the header, there is a section titled '全般' (General). This section contains several fields: 'ID\*' with the value '29ca944f-8318-493c-8d69-c92e6afd1c5a'; '名前' (Name) with the value '新規グループ', which is highlighted with a red rectangular box; '親グループ' (Parent Group) with the text '親グループはありません' and a pencil icon; 'プロフィール' (Profile) with the text '編集' and a pencil icon; 'ポリシーの割り当てなし' (No policy assignment) with a pencil icon; and '説明' (Description) with a large text area.

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

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。

※ Windows OS 向けエージェントインストーラーフルパッケージは、必ず最新のものをダウンロードしてご利用ください。

- 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。

※ 2023/07/20 時点では、以前のバージョン(Ver 12、Ver 11)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、必ず Ver13 用のものをダウンロードしてください。

- 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。

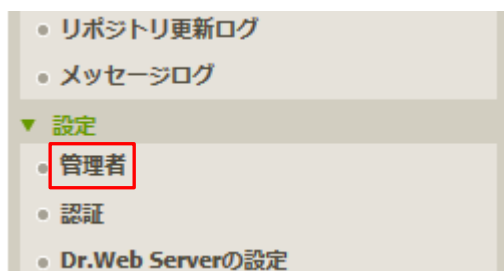
- 4) PC の再起動中に 6-2-2 の 6)~10)の手順を実行します。

※ 必ず、端末を Control Center 上で承認してください。

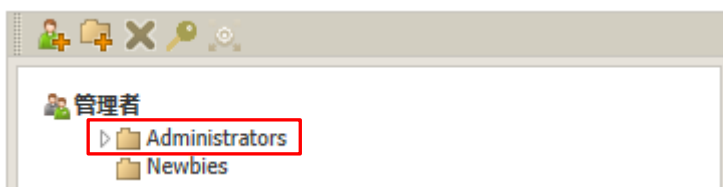
## 7. ケーススタディ

### 7.1 管理者(admin)パスワードの変更

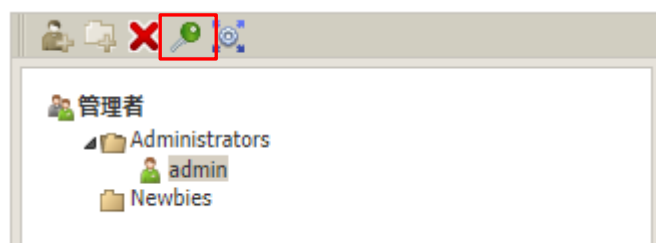
- 1) Control Center にログインします。
- 2) 「管理」メニューに移動します。
- 3) [設定]-[管理者]をクリックします。



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

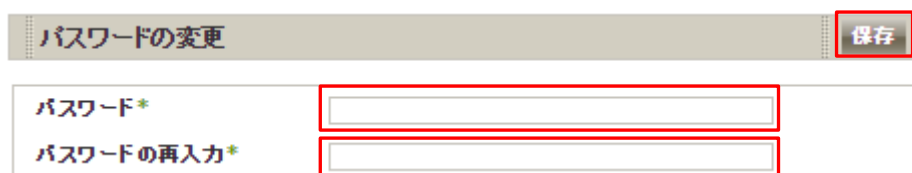


- 5) 「admin」を選択し、「パスワードの変更」アイコンをクリックします。



※ 「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」グループに割り当ててください。

- ※ ESS13 では、以前のバージョン(Ver12、Ver11)と同様に一つのグループに複数のライセンスキーを割り当てたり、逆に一つのライセンスキーに複数のグループを割り当て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割り当てることも可能です。ライセンスが割り当て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。

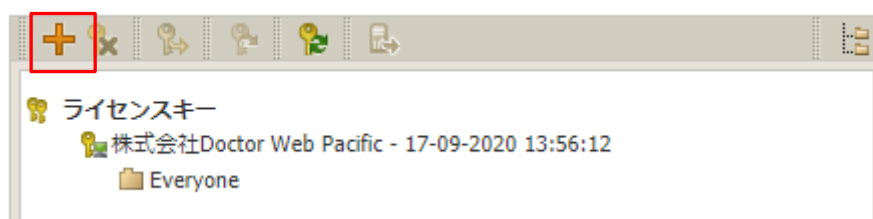
**【注意】**複数のライセンスを1つのグループに割り当てて利用する場合、各ライセンスでサポートされているコンポーネントのうち**共通するもののみが利用可能**となります。

- 1) Control Center 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
<input checked="" type="checkbox"/>  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

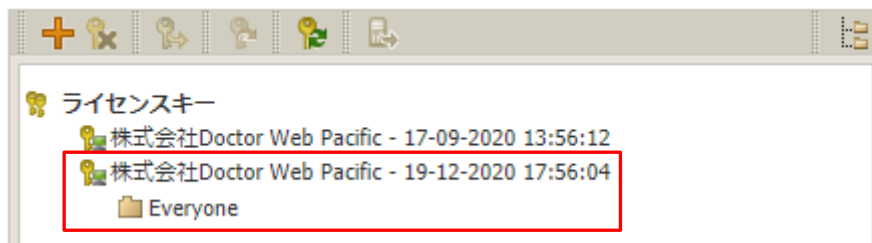
インポートされたキーで指定されている、インストールコンポーネントのリストは、現在のキーのリストとは異なります

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

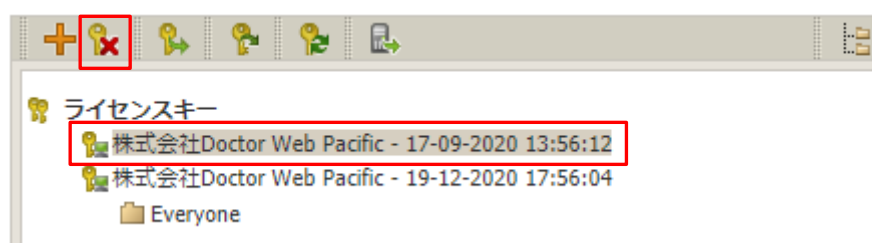
	現在のキー	割り当てるキー
<input checked="" type="checkbox"/>  Everyone	株式会社Doctor Web P...	株式会社Doctor Web P...
SpIDer Guard for Windows servers	インストール可能	インストール不可能

☒ 異なるもののみを表示

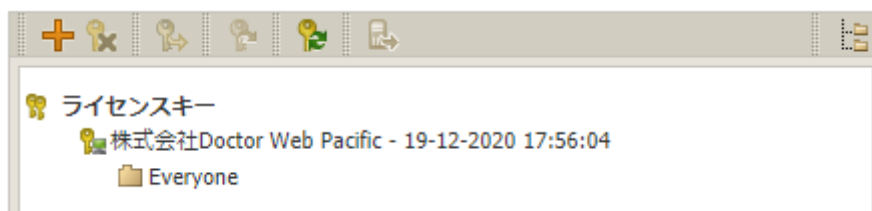
- 9) 画面中央の「ライセンスキー」ツリーに追加したライセンスの「登録名」と「ライセンス終了日」が表示されたこと、「Everyone」グループに割り当てられたことを確認します。



- 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ることがありますので、必ずライセンス更新後には「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

Dr.Web Agent for Windows 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(drwcds-certificate.pem)が、接続する ESS サーバのものか
- ESS サーバ、Dr.Web 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 Dr.Web Agent 間で使用するポートが閉じられていないか
- 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

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 drwcds-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>
```

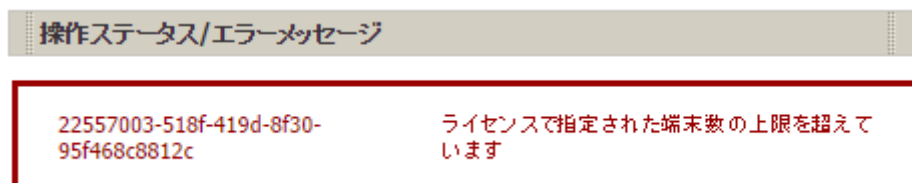
### 7.4 Dr.Web Agent for Windows の言語の変更

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) Control Center 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

Control Center 上で、「アンチウイルスネットワーク」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。

- Self-Protection
- 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 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 Control Center 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 をマスターイメージ作成用 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指定した SetupComplete.cmd を作成します。

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) Control Center 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および更新されたプログラム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 をマスターイメージ作成用 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指定した SetupComplete.cmd を作成します。

`drweb-13.0.3-202305110-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-13.0.3-202305110-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) Control Center 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 サーバはあるが、イメージ展開時に通信が不可能な場合

ESS サーバとの通信が可能となった状態で、各 PC から Dr.Web Agent for Windows 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 サーバの構築後に、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/](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。

ファイルをお送りいただいた後の弊社対応には時間をいただきますので、合わせて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) Control Center 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) Control Center 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) Control Center 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

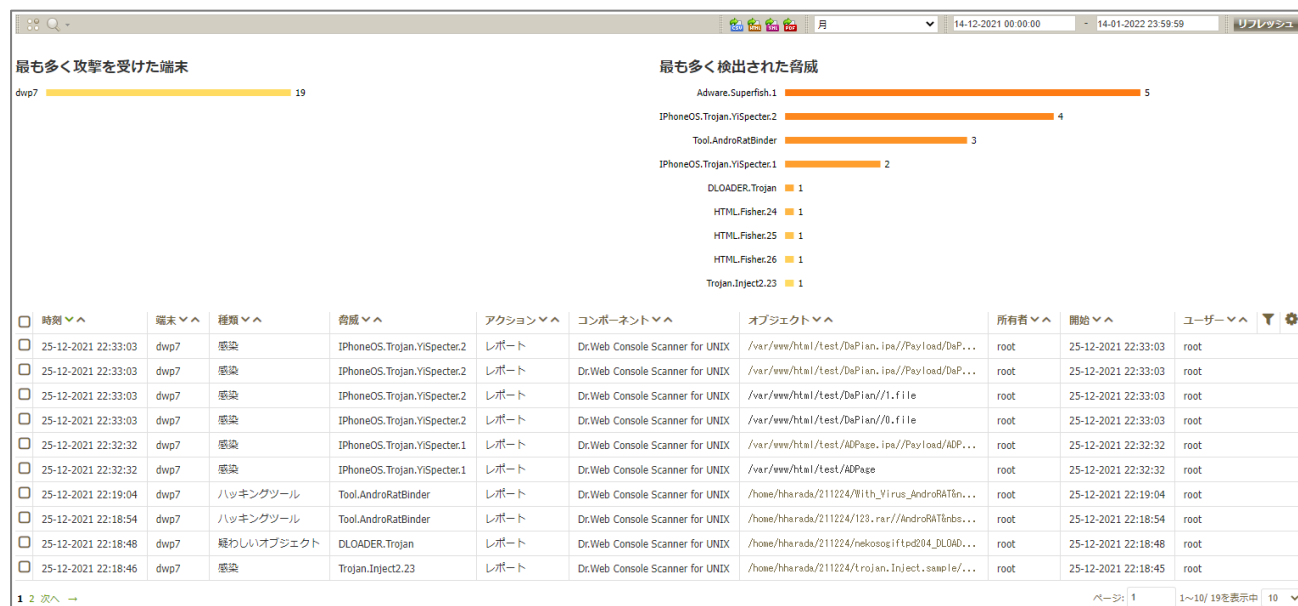
		①	②				③			④	⑤	⑥	
			CSV	HTML	PDF	月	14-12-2021 00:00:00			14-01-2022 23:59:59			リフレッシュ
端末	コンポーネント												
dwp7	Dr.Web Console Scanner for UNIX	21	15	0	1		0	0	0	0	0	2	12359
DESKTOP-SRKTBQO	SpIDer Mail for Windows	0	0	0	0		0	0	0	0	0	0	0
DESKTOP-SRKTBQO	SpIDer Gate for Windows workstations	208	0	0	0		0	0	0	0	0	0	0
DESKTOP-SRKTBQO	SpIDer Guard for Windows workstations	96500	0	0	0		0	0	0	0	0	0	1424041
VERIFICATION	SpIDer Mail for Windows	0	0	0	0		0	0	0	0	0	0	0
VERIFICATION	SpIDer Gate for Windows workstations	493	0	0	0		0	0	0	0	0	0	0
VERIFICATION	SpIDer Guard for Windows workstations	126713	0	0	0		0	0	0	0	0	0	14267501

1

ページ: 1 1~7/ 7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。



- **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。

※ メールファイルや zip ファイル等から脅威が検出され、隔離(または削除)を行なった場合、メールファイルや zip ファイル自身に対してはアクションとして「隔離」(または「削除」)が表示されますが、脅威が検出されたメールファイルや zip ファイル内のファイルについてはアクションとして「レポート」が表示されます。

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

### 7.12.1 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。

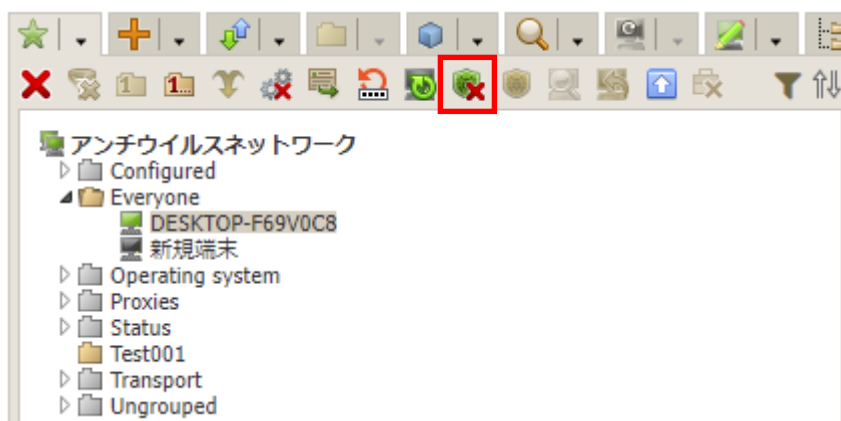
- Control Center 上から
- クライアント PC 上から

※ Control Center の「アンチウイルスネットワーク」メニュー内の「パーミッション」にて、「Dr.Web Agent をアンインストールする」が有効となっている必要があります。

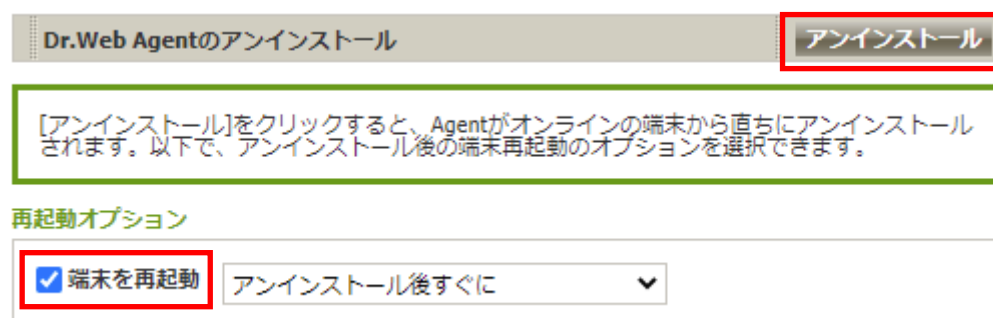
#### 7.12.1.1. Control Center 上からのアンインストール

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

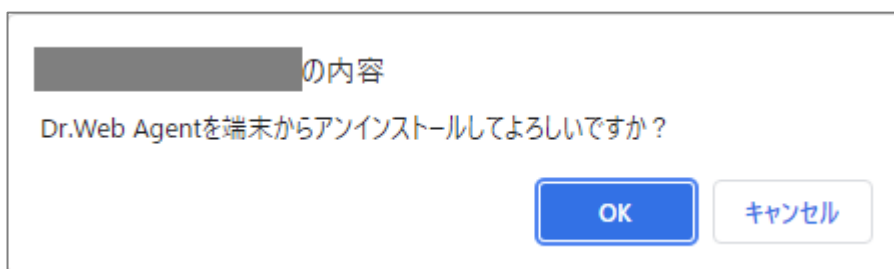
- 1) Control Center にログインします。
- 2) 「アンチウイルスネットワーク」メニュー中央のツリーから対象の端末を選択します。
- 3) ツリー上部の全般アイコン(星型のアイコン)をクリックし、下図の赤枠のアイコン(Dr.Web のアイコンに赤い×印がついたアイコン)をクリックします。



- 4) 右側に表示された「Dr.Web Agent のアンインストール」の画面にて「端末を再起動」のチェックを入れ、「アンインストール」ボタンをクリックします。



- 5) 以下のメッセージが表示されたら、「OK」をクリックします。

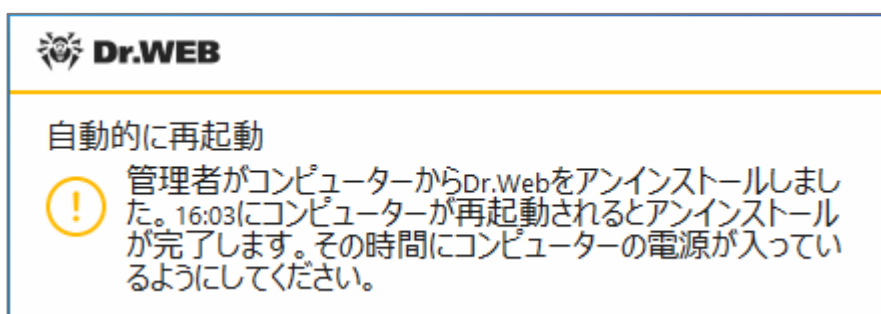


- 6) 以下のような表示がされたことを確認します。

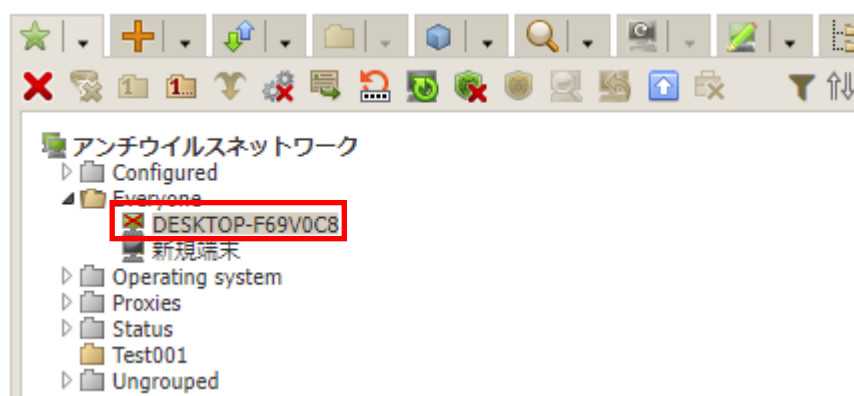


- 7) クライアント PC 上に以下のようなメッセージが表示されたら、PC を再起動してください。

※ メッセージ内には、以下のように再起動の予定時刻が表示されています。



- 8) Control Center 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 Control Center 上から端末を削除してください。

#### 7.12.1.2. 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、Control Center 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。

※ Control Center 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。

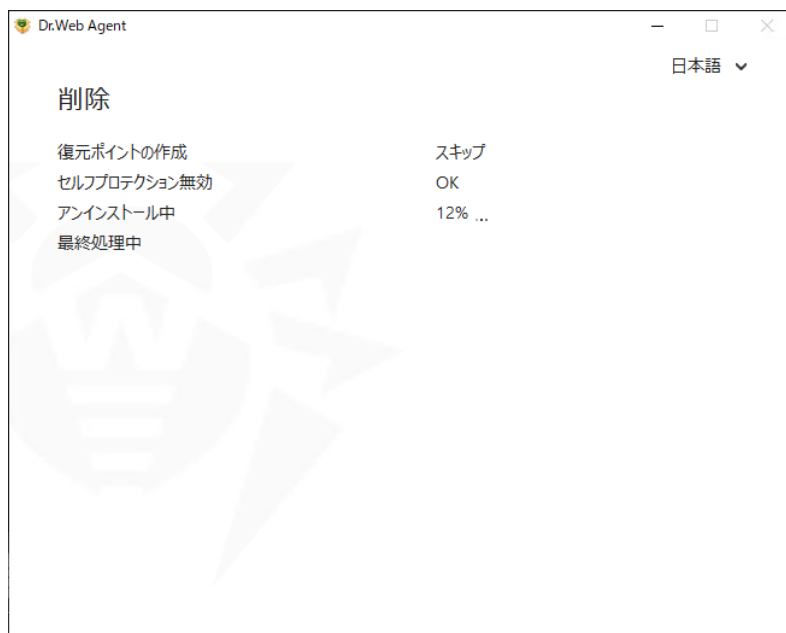
- 3) 以下の画面で「次へ」をクリックします。



- 4) 以下の画面で「削除」をクリックします。



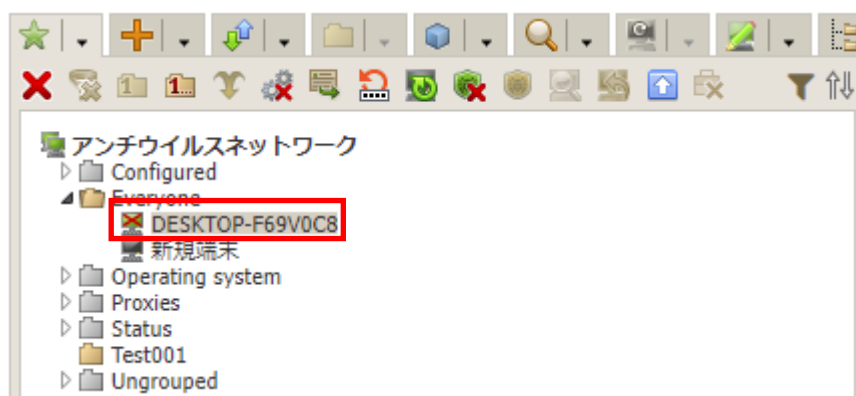
- 5) アンインストールが開始します。



- 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) Control Center 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 Control Center 上から端末を削除してください。

## 7.12.2 アンインストールに失敗する場合の対処

7.12.1 の手順でアンインストールができなかったり(Control Center 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](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 for Windows 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、削除ツール("drw\_remover.exe")を使用して、Dr.Web Agent for Windows をアンインストールした場合、他の方法と異なり Control Center 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。

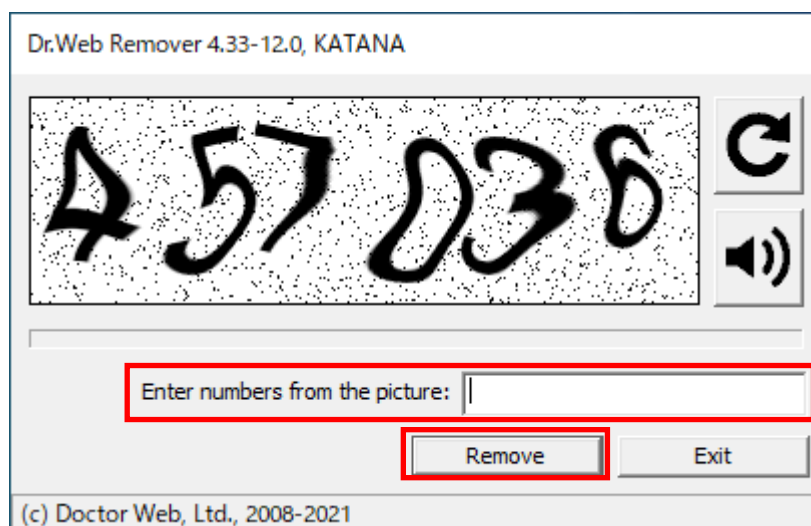
※ "drw\_remover.exe"は、都度ダウンロードしてください。ご利用中の Dr.Web Agent for Windows に未対応の"drw\_remover.exe"を使用すると、削除が適切に実行されない場合があります。

- 2) 当該端末上で 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。

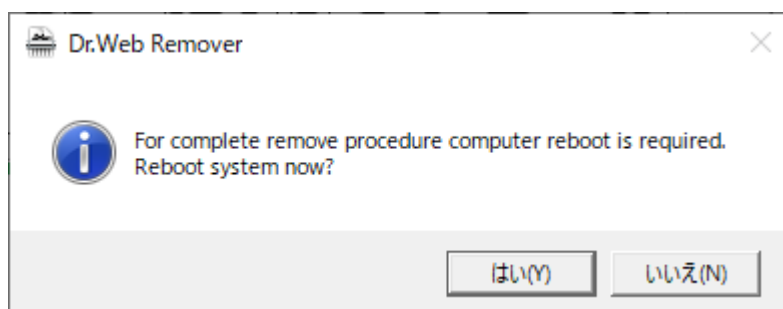
※ 「ユーザーアカウント制御」の画面が表示されたら「はい」をクリックしてください。

- 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。



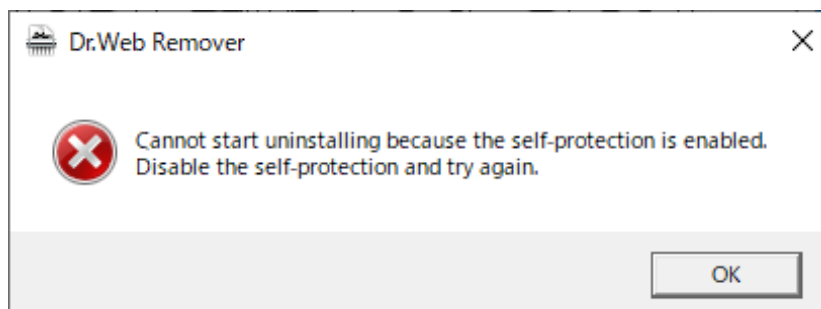


- 5) 以下の画面が表示されたら、「はい」をクリックして PC を再起動します。



※ 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 Control Center 上から端末を削除してください。

**【注意】**Self-Protection を無効にしていない場合には、「Remove」をクリックした後、以下のようなメッセージが表示されます。



お使いの製品の詳細な機能の説明や、利用方法は、各製品マニュアルをご参照ください。

また、製品のご利用について、ご質問やトラブル等がありましたら、下記 URL よりお気軽にお問い合わせください。

<https://support.drweb.co.jp/>

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](http://www.drweb.co.jp)